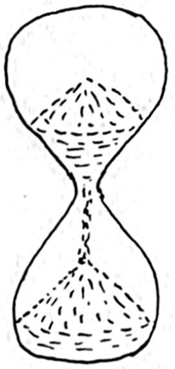
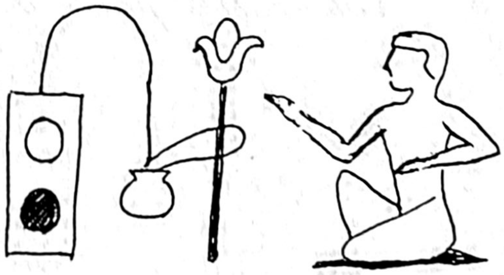
Extrait du cours d'algèbre [illegible]
donné par Cerezo à l'Univ. de Nice
(année univ. 90-91)

INTRODUCTION

LE FOND



L'algèbre, c'est l'art de "calculer", du latin calculus = l'un de ces petits cailloux qu'on faisait passer d'un tas sur un autre ; aujourd'hui, les cailloux sont souvent remplacés par des électrons, demain peut-être par des photons, et les règles de l'art se sont un peu perfectionnées au cours des siècles.



La question centrale de l'algèbre est la résolution des systèmes d'équations algébriques. C'est un souci ancien : dans un papyrus égyptien du musée de Berlin, datant de trois millénaires et demi, on trouve déjà, exprimé sous une forme géométrique, l'énoncé du problème : trouver deux nombres x et y tels que $x^2+y^2=100$, et $4x=3y$. Après un calcul peu explicite, le scribe conclut que $x=6$ et $y=8$. Aujourd'hui on citerait aussi une deuxième solution $x=-6$ et $y=-8$ (s'agissant de longueurs de champs, elle n'aurait guère plû à l'ancien scribe), mais le plus intéressant est qu'il n'y en a pas d'autre.

Plus généralement, un système d'équations algébriques s'écrit

$$P_1(x_1,\dots,x_n)=0\ ;\ P_2(x_1,\dots,x_n)=0\ ;\ \dots\ ;\ P_q(x_1,\dots,x_n)=0\,.$$

où $P_1, P_2, \dots, P_q$ sont des polynômes des variables $x_1,\dots,x_n$ (c'est-à-dire des sommes de produits de puissances de ces variables, affectés de coefficients que l'on prend dans un corps de nombres – voir plus loin des définitions plus claires), et l'on cherche quelles familles de nombres on peut substituer aux "inconnues" $x_1,\dots,x_n$ pour que les égalités écrites soient vraies. Les "nombres" avec lesquels on va calculer sont souvent les plus classiques : nombres entiers, rationnels, réels, ou complexes. Mais d'autres espèces de nombres sont utiles aussi, et il convient de dégager les règles de calcul les plus générales possibles.

Bien que les équations algébriques soient les plus élémentaires, ne faisant intervenir que des additions et des multiplications, leur résolution est un problème extrêmement difficile, même lorsqu'on se borne à calculer avec des nombres entiers ; dans ce cas on les appelle équations "diophantiennes", d'après Diophante, le premier à tenter leur étude systématique. Dix-sept ou dix-huit siècles plus tard, elles défient toujours l'esprit humain, malgré un immense répertoire d'idées et de méthodes accumulées pour les dénouer. Une de ces méthodes, et des plus anciennes, est d'inventer de nouveaux corps de nombres où l'on va chercher des solutions, et qui sont plus vulnérables parce que fabriqués pour cela. C'est ainsi qu'on a

fabriqué les nombres <u>rationnels</u>, puis les <u>réels</u> et les complexes, bien d'autres encore dont on verra quelques exemples. Les adjectifs ici soulignés, imposés par l'usage, ne doivent pas trop faire illusion : ils témoignent surtout que l'on est assez habile à jouer avec ces nombres pour qu'ils nous paraissent les plus naturels.

Dans ce cours, on n'envisage que <u>deux cas particuliers</u> de systèmes d'équations algébriques, qui sont à la fois les plus faciles et les plus utiles :

1) il y a <u>une seule</u> inconnue x, et on a donc à résoudre des équations du type $P(x)=0$, où P est un polynôme d'une seule variable. C'est l'objet de la deuxième partie.

2) il y a autant d'inconnues et d'équations que l'on veut, mais tous les polynômes sont de degré 1 ; c'est ce qu'on appelle un système <u>linéaire</u>. L' "algèbre linéaire" et son application à la géométrie constituent la troisième partie.

Avant de les aborder, il y a lieu de préciser les nombres avec lesquels on va ensuite calculer, et c'est ce qu'on fait dans la première partie. Enfin se dégage des calculs l'importance de certaines structures sous-jacentes, les "structures algébriques" de base : groupes, anneaux, corps, espaces vectoriels. Les deux dernières sont, par nécessité, largement explicitées au cours de ces trois parties ; une étude plus systématique des deux premières fait l'objet de la quatrième partie.

TABLE DES MATIÈRES

INTRODUCTION : Le fond. La forme. Index des matheux. Alphabet grec.

PREMIÈRE PARTIE : DES NOMBRES

1 - LES NOMBRES ENTIERS :
Ⓐ Les entiers naturels, Ⓑ La division dans l'anneau des entiers, Ⓒ Décomposition en facteurs premiers, Ⓓ Les entiers "modulo n".

2 - DES ENTIERS AUX COMPLEXES :
Ⓐ Jusqu'à l'équation du second degré, Ⓑ Calculs dans le corps des complexes.

3 - GROUPES, ANNEAUX, CORPS :
Ⓐ Groupes, Ⓑ Anneaux et corps, Ⓒ Equivalences, partitions, ensembles-quotients.

DEUXIÈME PARTIE : DES POLYNÔMES

4 - L'ANNEAU DES POLYNÔMES :
Ⓐ Formalités, Ⓑ Polynôme et fonction polynôme.

5 - THÉORIE DE LA DIVISION :
Ⓐ Euclide, Bezout, Gauss, Ⓑ Factorisation irréductible, Ⓒ Une autre division.

6 - APPLICATION AUX EQUATIONS ALGÉBRIQUES :
Ⓐ Factorisation et interpolation, Ⓑ Racines multiples, Ⓒ Relations entre coefficients et racines, Ⓓ Dernières remarques sur la division.

7 - LE CORPS DES FRACTIONS RATIONNELLES :
Ⓐ Fractions rationnelles et fonctions rationnelles, Ⓑ Décomposition en éléments simples, Ⓒ Pratique de la décomposition ($K = \mathbb{R}$ ou $\mathbb{C}$).

TROISIÈME PARTIE : ALGÈBRE LINÉAIRE

8 - SYSTÈMES LINÉAIRES - LA MÉTHODE DE GAUSS :
Ⓐ Systèmes linéaires, Ⓑ Un exemple de la méthode de Gauss, Ⓒ Dernières remarques

9 - ESPACES VECTORIELS :
Ⓐ Le vocabulaire et les idées de base, Ⓑ Le théorème fondamental en dimension finie, Ⓒ Rang et dimension, somme directe et supplémentaires, Ⓓ Espace-vectoriel produit, espace-vectoriel quotient.

10 - APPLICATIONS LINÉAIRES :
Ⓐ Applications linéaires, noyaux et images, Ⓑ Rangs et dimensions, Ⓒ L'anneau End(E) et le groupe GL(E)

11 - CALCUL MATRICIEL
Ⓐ Matrices et applications linéaires, Ⓑ Rang, équivalence, et transposition, Ⓒ Changements de bases, Ⓓ Inversion par la méthode de Gauss

12 - DÉTERMINANTS
Ⓐ Signature d'une permutation, Ⓑ Formes multilinéaires alternées, Ⓒ Déterminants, Ⓓ Calcul des déterminants et des inverses.

13 - SYSTÈMES LINÉAIRES - ROUCHÉ ET CRAMER :
Ⓐ Retour sur les systèmes linéaires, Ⓑ Commentaires et exemples.

14 - TRACE, ÉLÉMENTS PROPRES, DUALITÉ
Ⓐ Trace, Ⓑ Valeurs propres et vecteurs propres, Ⓒ Dualité.

15 - GÉOMÉTRIE AFFINE
Ⓐ Principe de la géométrie affine, Ⓑ Calculs dans un repère, Ⓒ Thalès, le parallélogramme et les dilatations, Ⓓ Quelques énoncés classiques.

⟶

QUATRIÈME PARTIE : STRUCTURES ALGÉBRIQUES

16 - GROUPES :

Ⓐ Notions de base et exemples, Ⓑ Groupes-quotients, Ⓒ Produit semi-direct de groupes, Ⓓ Générateurs, groupe dérivé, groupes cycliques.

17 - ACTIONS DE GROUPES :

Ⓐ Généralités, Ⓑ Le groupe affine, Ⓒ Le groupe symétrique

18 - ANNEAUX :

Ⓐ Anneaux, idéaux, Ⓑ La division dans un anneau principal

APPENDICES

I - L'AXIOME DU CHOIX

II - LES GROUPES FINIS SIMPLES

III - LES CORPS FINIS

IV - GÉOMÉTRIE AXIOMATIQUE

V - NOMBRES P-ADIQUES

VI - LES GROUPES DE LA PHYSIQUE

Si la résolution des équations algébriques est ici le fil conducteur, les idées, méthodes et techniques développées ne manquent pas d'être utiles dans toutes sortes de contextes de caractère scientifique ou technique, et on y fera évidemment quelques allusions.

Enfin on trouvera dans quelques appendices de quoi satisfaire une légitime curiosité sur quelques uns des abîmes qu'on aura été amené à côtoyer.

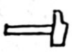
LA FORME

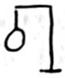
L'ensemble des quatre parties se compose de 18 chapitres, de longueurs inégales, eux-mêmes divisés en paragraphes, notés A, B, C,... Chacun se compose de "numéros" 1, 2, 3,... qui développent une ou deux idées importantes. Ainsi la référence 14-B-5 signifie le numéro 5 du paragraphe B du chapitre 14.

Le texte n'est évidemment pas partout d'égale importance. Pour aider à distinguer l'essentiel de l'accessoire et le luxe du nécessaire, les signes suivants, placés en marge d'un numéro, ou du corps de son texte, seront utilisés systématiquement:

"Noyau": un point de base, constituant du corps de ce cours; à retenir sans faute.

"Clé": contient une idée riche, qui en ouvre beaucoup d'autres; il faut s'en pénétrer pour pouvoir l'utiliser au moment opportun.

 "Marteau": technique de calcul mécanique; à bien rôder et maîtriser complètement et fiablement.

 "Potence": signale une erreur pendable; à noter pour l'éviter absolument.

"Promenade": développement ou illustration de ce qu'on vient de dire; à lire certainement, pour comprendre, mais dont le contenu n'est pas forcément à retenir entièrement.

"Méditation", placée là pour inviter à la réflexion, aider à une compréhension plus profonde, une perspective plus vaste; à lire sans souci de tout retenir (d'ailleurs souvent hors programme).

Autres signes utilisés dans le texte :

Des crochets ⌜---⌟ entourent un passage tout-à-fait facultatif : développement hors programme, ou au contraire exemple traité dans le détail.
Un carré ■ est utilisé pour signaler la fin d'une démonstration.
Des étoiles (*), (**), ... en marge d'une formule ou d'une équation évitent d'avoir à la répéter lorsqu'on la citera quelques lignes plus bas.
Signalons aussi ici le sens des symboles courants qui nous servent souvent d'abréviations (et se conjuguent mentalement) :

$\forall$ se lit "pour tout", "quel que soit"
$\exists$ " "il existe" ; $\exists 1$ "il existe un et un seul"
$\in$ " "appartient à", "appartenant à", "dans"
$\subset$ " "inclus dans", "partie de"
$\emptyset$ " "l'ensemble vide" (rien à voir avec zéro)

La rédaction est volontairement très variée, certaines démonstrations étant écrites de la façon la plus détaillée, d'autres tout juste indiquées en style "télégraphique".

Les énoncés "soulignés" portent différents noms, que l'on emploie ici avec une certaine indifférence. Toutefois le terme le plus banal est "proposition", tandis que "théorème" est réservé à un résultat particulièrement important, "lemme" à un résultat intermédiaire préparant la démonstration d'un théorème, et "corollaire" à une conséquence facile d'un autre énoncé déjà vu.

PETIT INDEX DES PRINCIPAUX MATHEUX CITÉS

ABEL Niels Henrik, 1802/1829, norvégien, Oslo, mort de tuberculose et d'épuisement.
ALEMBERT Jean Le Rond d', 1717/1783, physicien et philosophe français, Paris.
ARCHIMÈDE, 287/212 av. J.C., ingénieur grec, Syracuse, tué par un soldat romain.
BEZOUT Étienne, 1730/1783, français.
CARDAN(O) Gerolamo, 1501/1576, médecin italien, Padoue, Pavie, Milan, Bologne
CAUCHY Augustin Louis, 1789/1857, français, Paris, père de dix-huit enfants.
CRAMER Gabriel, 1704/1752, suisse, Genève.
DESARGUES Gérard, 1591/1661, ingénieur français, Lyon.
DESCARTES René, 1596/1650, philosophe français, Hollande.
DIOPHANTE, IIe/IIIe siècle, grec, Alexandrie (d'Egypte)
EUCLIDE, IVe/IIIe siècle av. J.C., grec, Alexandrie
FERMAT, Pierre de, 1601/1665, magistrat français, Toulouse
GALOIS Evariste, 1811/1832, français, Paris, tué en duel par un mari jaloux.
GAUSS Carl Friedrich, 1777/1855, allemand, Göttingen, "le prince des mathématiciens".
HILBERT David, 1862/1943, allemand, Göttingen, a le plus influencé les maths du XXe siècle.
KRONECKER Leopold, 1823/1891, allemand, Berlin.
LAGRANGE Joseph-Louis, 1736/1813, physicien franco-italien, Turin, Berlin, Paris.
LEIBNIZ Gottfried Wilhelm, 1646/1716, philosophe allemand, Hanovre, a écrit plus de 200.000 pages.
MOIVRE Abraham de, 1667/1754, franco-anglais, Londres.
NEWTON Isaac, 1642/1727, physicien anglais, Cambridge, Londres, a reçu une pomme sur la tête
NOETHER Emmy, 1882/1935, allemande, Erlangen, la première femme qui ait marqué l'algèbre, ... [ou plutôt la deuxième.
PAPPUS, IVe siècle, grec, Alexandrie
PEANO Giuseppe, 1858/1932, italien, Turin.
PYTHAGORE, VIe siècle av. J.C., mystique grec, Samos, Crotone (Italie du Sud)
TAYLOR Brook, 1685/1731, anglais, Cambridge.
THALÈS, VIIe/VIe siècle av. J.C. grec, Milet (aujourd'hui en Turquie).

ALPHABET GREC

Les matheux ont souvent besoin, pour la clarté, d'un alphabet de réserve.
En hommage aux pères fondateurs, le plus souvent utilisé est le grec, de 24 lettres.
Seules les minuscules, et les rares majuscules distinctes des latines, sont employées.

α	A	alpha	ι	I	iota	ρ	P	rhô
β	B	bèta	κ	K	kappa	σ	Σ	sigma
γ	Γ	gamma	λ	Λ	lambda	τ	T	tau
δ	Δ	delta	μ	M	mu	υ	U	upsilon
ε	E	èpsilon	ν	N	nu	φ	Φ	phi
ζ	Z	zéta	ξ	Ξ	ksi	χ	X	chi (prononcer ki)
η	H	héta	o	O	omicron	ψ	Ψ	psi
θ	Θ	théta	π	Π	pi	ω	Ω	oméga

PREMIÈRE PARTIE : DES NOMBRES

« Dieu a créé les nombres entiers ... les hommes, ensuite, ont crû bon d'inventer le reste ... » (adapté de Kronecker)

Tout commence avec l'arithmétique, dont on pose les bases au chapitre 1. En même temps, cette étude de l'anneau des entiers nous fournit le prototype de notions et de méthodes qui s'appliqueront ensuite à la résolution des équations algébriques, à la deuxième partie. L'usage systématique des mêmes idées donne le chapitre 18.

Au chapitre 2 on rappelle la construction des corps de nombres classiques, et les techniques de calculs particulières aux nombres complexes. Leur application aux équations algébriques de petit degré donne les fameuses formules de résolution "par radicaux."

On a concentré en un court chapitre 3 un paquet de définitions plus ou moins inévitables, dont on fera inopinément usage dans toute la suite.

CHAPITRE 1 : LES NOMBRES ENTIERS

« Unitas est secundum quam entium quodque dicitur unum. Numerus autem, ex unitatibus composita multitudo. » (édition gréco-latine des "Éléments" d'Euclide, livre VII, Paris 1573 — non distribué dans les grandes surfaces)

(A) LES ENTIERS NATURELS

1 - C'est 0, 1, 2, 3, 4, 5, ... On suppose ici partager avec le lecteur une connaissance intuitive des entiers naturels (« huit fois sept font cinquante-six »...), dont on note $\mathbb{N}$ l'ensemble, infini ordonné et muni de deux opérations "connues", l'addition et la multiplication (ou encore "somme" et "produit"). On se contente des deux remarques suivantes :

2 - Les opérations ne sont pas indépendantes ; en fait la multiplication se définit comme une addition répétée : p fois q égale $\underbrace{q+q+\cdots+q}_{p \text{ fois}}$;
de même il suffit de savoir ajouter 1 pour définir l'addition :
$p+q = p+\underbrace{1+1+\cdots+1}_{q \text{ fois}}$. A vrai dire, cela n'est pas si clair : est-ce que le "nombre de fois" dans "p fois" est bien la même notion que l'entier p, élément de $\mathbb{N}$? Et comment vérifie-t-on les propriétés bien connues de "commutativité" ($p+q=q+p$; $pq=qp$), d'"associativité" ($(p+q)+r=p+(q+r)$, $(pq)r=p(qr)$) et de "distributivité" ($p(q+r)=pq+pr$) de ces opérations ?

Pourtant ces idées permettent de reconstituer $\mathbb{N}$ et ses propriétés à partir de la seule notion d'"ajouter 1", autrement dit l'application qui à un entier fait correspondre son "suivant" : $p \mapsto p+1$. Ceci a été formalisé par Peano, qui arrive à "tout" déduire de quelques axiomes. On ne s'étend pas ici là-dessus, sauf à la remarque qui suit, à propos du dernier de ces axiomes, le fameux "principe de récurrence."

3 - Le principe de récurrence, sous sa forme la plus courante, dit ceci :

(*) Si on considère une famille d'assertions $\mathcal{P}_n$ numérotées à l'aide d'entiers ($n \in \mathbb{N}$), que la première $\mathcal{P}_0$ est vraie, et qu'il est vrai que chacune implique la suivante ($\forall n \in \mathbb{N}, \mathcal{P}_n \Rightarrow \mathcal{P}_{n+1}$), alors elles sont toutes vraies : $\forall n \in \mathbb{N}, \mathcal{P}_n$.

Une forme affaiblie du même principe dit ceci :

(**) Avec les mêmes notations, si $\mathcal{P}_0$ est vraie et si la véracité des n premières assertions implique celle de la suivante ($\forall n \in \mathbb{N}, \{\forall k \in \mathbb{N}, k \leq n \Rightarrow \mathcal{P}_k\} \Rightarrow \mathcal{P}_{n+1}$), même conclusion : $\forall n \in \mathbb{N}, \mathcal{P}_n$.

En fait ces deux "principes" sont logiquement équivalents à la propriété suivante de l'ensemble ordonné $\mathbb{N}$, que l'on pose comme axiome :

(***) Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Preuve : il est clair que (*) est plus fort que (**). Admettons (**) et montrons (***). Soit E une partie de $\mathbb{N}$ qui n'a pas de plus petit élément. On'appartient donc pas à E (car 0 est plus petit que tout autre entier). Considérons pour chaque entier n l'assertion $\mathcal{P}_n : n \notin E$. $\mathcal{P}_0$ est donc vrai ; de plus supposons $\mathcal{P}_k$ vrai pour tout $k \leq n$: soit $k \leq n \Rightarrow k \notin E$. Alors $n+1 \notin E$ (sinon $n+1$ serait le plus petit élément de E), autrement dit $\mathcal{P}_{n+1}$ est vrai. Par (**) on conclut alors : $\forall n, \mathcal{P}_n$, soit $n \notin E$, et E est donc vide.

Enfin montrons que (***) implique (*), en considérant l'ensemble $E = \{n \in \mathbb{N} \mid \mathcal{P}_n \text{ faux}\}$. Si $E \neq \emptyset$, soit n_0 son plus petit élément ; $n_0 \neq 0$ puisque $\mathcal{P}_0$ est vrai et $\mathcal{P}_{n_0}$ est faux. Donc n_0 a un <u>précédent</u> : $n_0 = n+1$; et $n < n_0$ implique $n \notin E$, donc $\mathcal{P}_n$ vrai. Mais alors $\mathcal{P}_{n+1}$ est vrai aussi, donc $n_0 = n+1 \notin E$, ce qui est absurde. Par suite $E = \emptyset$, autrement dit $\forall n, \mathcal{P}_n$. ∎

Dans la suite, on admet la propriété (***) des entiers, et on se permet donc un usage systématique des "raisonnements par récurrence" (*) ou (**).

4 - On rajoute aux entiers naturels leurs "<u>opposés</u>" $-0 = 0, -1, -2, -3, \ldots$ pour former l'ensemble $\mathbb{Z}$ des entiers "relatifs" (on dira ici les <u>entiers</u> tout court) : $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, auquel on étend l'ordre et les opérations de $\mathbb{N}$ de la façon "bien connue", ce qui fait de $\mathbb{Z}$ un "anneau" (cf. chapitre 3, §B) commutatif, totalement ordonné et "<u>intègre</u>" : $ab = 0 \Rightarrow a = 0$ ou $b = 0$ (si $a, b \in \mathbb{N}$, cela résulte de la définition du produit...) Insistons ici sur la "règle des signes" : + fois + = − fois − = + ; + fois − = − fois + = −.

Remarquons une conséquence précieuse du principe de récurrence :

<u>Lemme</u> : $\forall n \in \mathbb{N}^*, \forall N \in \mathbb{Z}, \exists 1\, p \in \mathbb{Z}, pn \leq N < (p+1)n$ $\quad (\mathbb{N}^* = \mathbb{N} - \{0\})$

En effet si $N \in \mathbb{N}$, considérons $E = \{q \in \mathbb{N} \mid qn > N\}$. Comme $N+1 \in E$ puisque $n \geq 1$, E n'est pas vide ; soit p' son plus petit élément. $p' \neq 0$ puisque $N \in \mathbb{N}$, donc p' a un précédent : $p' = p+1$ avec $p \in \mathbb{N}$. Si maintenant $N \in -\mathbb{N}$, le raisonnement ci-dessus s'applique à $-N$, d'où $p \in \mathbb{N}$ tel que $pn \leq -N < (p+1)n$, donc $(-p-1)n < N \leq -pn$, et c'est $-p-1$ ou $-p$ qui convient... ∎

⌜En fait il s'agit ici de l'existence de la "<u>partie entière</u>" p d'un nombre rationnel $\frac{N}{n}$.⌟

On tire de ce lemme un résultat fondamental pour la suite :

5 - "<u>Théorème de la division euclidienne</u>"

$$\forall (a,b) \in \mathbb{Z}^2, b > 0, \exists 1\, (q, r) \in \mathbb{Z}^2, \ a = bq + r \ \text{et} \ 0 \leq r < b$$

(« Pour tout couple a, b d'entiers, avec b positif strictement, il existe un et un seul couple q, r d'entiers tels que a soit égal à q fois b plus r, et que r soit positif ou nul, et strictement plus petit que b. » ; q et r s'appellent le <u>quotient</u> et le <u>reste</u> de la division euclidienne de a par b.

Preuve : le lemme 4 fournit q tel que $qb \leq a < (q+1)b$, d'où $0 \leq a - bq < b$, et il suffit de poser $r = a - bq$; l'unicité se voit en "remontant" le calcul. ∎

Il s'agit bien sûr de la division "avec reste" de l'école primaire, et la connaissance de la "table de multiplication" à base dix fournit l'<u>algorithme</u> connu :

$$\begin{array}{r|l} 3.784 & 7 \\ \cline{2-2} 28 & 540 \\ 04 & \\ 4 & \end{array}$$

, soit $\underbrace{3.784}_{a} = \underbrace{7}_{b} \times \underbrace{540}_{q} + \underbrace{4}_{r}$,

qui s'adapte aussi au cas $a<0$, mais attention : de $-3.784 = 7.(-540)-4$, on tire $-3.784 = 7.(-541)+3$, et on a $q=-541$ et $r=3$ lorsqu'on a pris $a=-3.784$ et $b=7$.

Lorsque le reste r de la division de a par b est nul, on dit que "b divise a", ou encore que "a est multiple de b" (dans ce cas $a=bq$), et on notera ici cette propriété : " $b|a$ ".

(B) LA DIVISION DANS L'ANNEAU DES ENTIERS

1- On appelle idéal de l'anneau $\mathbb{Z}$ une partie I non vide de $\mathbb{Z}$, stable par différences et par multiples, soit :
$$\begin{cases} \forall a,b\in I,\ a-b\in I & (I-I\subset I) \\ \forall a\in I, \forall p\in\mathbb{Z},\ pa\in I & (\mathbb{Z}.I\subset I) \end{cases}$$
Tout idéal contient 0 (car $I\neq\emptyset$, donc $\exists a\in I$, et $a-a=0\in I$), est stable par changement de signe ($a\in I$ et $0\in I \Rightarrow 0-a=-a\in I$), et par somme ($a\in I$ et $b\in I \Rightarrow -b\in I$, puis $a-(-b)=a+b\in I$). La partie à un seul élément $\{0\}$ est un idéal.

L'intersection de deux (ou plus) idéaux est un idéal, de même que leur somme (et non leur réunion !) : $I+J=\{a+b \mid a\in I, b\in J\}$.

2- Si $a\in\mathbb{Z}$, l'ensemble des multiples de a forme un idéal, noté I_a, ou encore $\langle a\rangle$, ou même $a.\mathbb{Z}$, et appelé l'idéal engendré par a.
De même, si $a_1,a_2,\dots,a_p\in\mathbb{Z}$, $I_{a_1}+I_{a_2}+\dots+I_{a_p}$ est un idéal : c'est l'ensemble des "combinaisons" de $a_1,a_2,\dots,a_p$ à coefficients entiers, c'est-à-dire l'ensemble de tous les entiers de la forme $u_1a_1+\dots+u_pa_p$, avec $u_1,\dots,u_p\in\mathbb{Z}$. On le note $I_{a_1,\dots,a_p}$ ou encore $\langle a_1,\dots,a_p\rangle$ et on l'appelle "l'idéal engendré par $a_1,\dots,a_p$." On dit encore que l'ensemble $\{a_1,\dots,a_p\}$ en est un "système de générateurs".

Si un idéal I admet un seul générateur a, soit $I=\langle a\rangle$, on dit qu'il est monogène. Par exemple $\{0\}$ est engendré par 0 : $I_0=\langle 0\rangle=\{0\}$; l'ensemble des entiers pairs est un idéal monogène : c'est I_2.
Le générateur d'un idéal monogène est unique au signe près : si $I_a=I_b$, c'est que $a=pb$ et $b=qa$, avec $p,q\in\mathbb{Z}$, d'où $a(pq-1)=0$, et si $a\neq 0$, $pq=1$, donc p et q valent ±1 ; si $a=0$, b aussi. ■

3- Théorème : Tout idéal de $\mathbb{Z}$ est monogène

Preuve : Soit I un idéal de $\mathbb{Z}$. Si $I=\{0\}$, $I=I_0$. Sinon $I^+=I\cap\mathbb{N}^*$ est non vide, car I contient un élément $a\neq0$, donc aussi $-a$, et a ou $-a$ appartient à $\mathbb{N}^*$.
Soit b le plus petit élément de I^+. Alors $I=I_b$, car si $a\in I$, on a par division euclidienne de a par $b>0$: $a=bq+r$ avec $0\le r<b$. Mais $a,b\in I$, donc $bq\in I$, puis $r=a-bq\in I$. Si $r\neq0$, $r\in I^+$ et $r<b$, ce qui est absurde. Donc $r=0$, et a est un multiple de b. ■

4- Soient $a_1, \dots, a_p$ des entiers, et b un diviseur commun : $b|a_1, b|a_2, \dots, b|a_p$. Alors b divise toute combinaison $u_1a_1 + \dots + u_pa_p$ ($u_1, \dots, u_p \in \mathbb{Z}$), et la réciproque est immédiate. Par le théorème 3, il existe d, d'ailleurs unique au signe près, tel que $\langle a_1, \dots, a_p \rangle = \langle d \rangle$, autrement dit tel que toute combinaison de $a_1, \dots, a_p$ est un multiple de d, et réciproquement.
En particulier d est un diviseur commun de $a_1, \dots, a_p$, et tout diviseur commun divise d. On appelle d le <u>plus grand commun diviseur</u> (p.g.c.d.) de $a_1, \dots, a_p$, et on le notera ici $a_1 \wedge \dots \wedge a_p$. ("plus grand" au sens que c'est un multiple de tous les autres).

Par exemple $4 \wedge 6 = 2$, car $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.

Le p.g.c.d. n'est défini qu'au signe près, et on pourra, pour le définir complètement, poser qu'un p.g.c.d. est toujours ≥ 0 (donc un entier naturel).
Il est clair que pour tout entier a, $a \wedge 0 = a$ et $a \wedge 1 = 1$.
Il est clair aussi que $a \wedge b = b \wedge a$, et que $a_1 \wedge a_2 \wedge \dots \wedge a_p = (\dots((a_1 \wedge a_2) \wedge a_3) \wedge \dots) \wedge a_p$ (propriété d' "associativité" des p.g.c.d.)

5- Si $d = a_1 \wedge \dots \wedge a_p$, en particulier $d \in \langle a_1, \dots, a_p \rangle$, autrement dit :

(*) <u>$\forall a_1, \dots, a_p \in \mathbb{Z}, \exists u_1, \dots, u_p \in \mathbb{Z}, \quad u_1a_1 + \dots + u_pa_p = a_1 \wedge \dots \wedge a_p$</u>

("<u>identité de Bezout</u>")

On dit que des entiers $a_1, \dots, a_p$ sont <u>premiers entre eux</u> s'ils n'ont pas de diviseur commun non trivial, autrement dit si $a_1 \wedge \dots \wedge a_p = 1$.

<u>Proposition (identité de Bezout)</u> : $\forall a_1, \dots, a_p \in \mathbb{Z}$

<u>$a_1 \wedge \dots \wedge a_p = 1 \iff \exists u_1, \dots, u_p \in \mathbb{Z}, \quad a_1u_1 + \dots + a_pu_p = 1$</u>

Preuve : $\Rightarrow$ est clair ; réciproquement si $1 \in \langle a_1, \dots, a_p \rangle = I$, I contient tous les multiples de 1, donc $I = \mathbb{Z} = \langle 1 \rangle$. ∎

En particulier pour deux entiers a et b, il est équivalent de dire qu'ils sont premiers entre eux, que leur pgcd vaut 1, qu'ils n'ont pas de diviseur commun (autre que ± 1), ou encore qu'il existe des entiers u et v tels que <u>$au + bv = 1$</u>.

Par exemple $18 \wedge 35 = 1$, puisque $2.18 - 1.35 = 1$.

Résoudre une "équation de Bezout" c'est trouver pour $a_1, \dots, a_p$ donnés toutes les familles d'entiers $u_1, \dots, u_p$ solutions de (*). Par exemple l'équation de Bezout $6u + 10v + 15w = 1$ a la solution $u = 1, v = 1, w = -1$ (ce qui prouve déjà que $6 \wedge 10 \wedge 15 = 1$). Mais $u = 6, v = 1, w = -3$ est une autre solution.

On donne au numéro suivant un algorithme de calcul d'un pgcd et d'une solution particulière d'une équation de Bezout. L'associativité implique qu'il suffit de savoir traiter le cas de deux entiers a et b.

6- L'algorithme d'Euclide

Remarquons que si $a = bq + r$, les diviseurs communs de a et b sont les mêmes que ceux de b et r ; en particulier $a \wedge b = b \wedge r$. Effectuons alors les divisions euclidiennes successives (comme $a \wedge b = a \wedge (-b)$, on peut supposer $b > 0$) :

$$a = bq_1 + r_1 \ , \quad 0 \leq r_1 < b$$

si $r_1 \neq 0$, $\quad b = r_1 q_2 + r_2 \ , \quad 0 \leq r_2 < r_1$

. . . . .

si $r_{n-1} \neq 0$, $\quad r_{n-2} = r_{n-1} q_n + r_n \ , \quad 0 \leq r_n < r_{n-1}$

Comme $b = r_0 > r_1 > r_2 > \dots > r_n$, "ça s'arrête", c'est-à-dire qu'il existe un entier n tel que $r_{n+1} = 0$ (encore une forme du principe de récurrence : l'ensemble des restes non nuls ainsi obtenus a un plus petit élément, éventuellement $r_0 = b$). Il vient alors : $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-1} \wedge r_n = r_n$ puisque $r_{n-1} = r_n q_n$.

<u>Le pgcd de a et b est donc le dernier reste non nul de cette suite de divisions euclidiennes.</u> Exemple : soit à calculer $2.244 \wedge 1134$

$$\begin{array}{r|l} 2.244 & 1134 \\ \hline 1.110 & 1 \end{array} \ , \quad \begin{array}{r|l} 1134 & 1110 \\ \hline 24 & 1 \end{array} \ , \quad \begin{array}{r|l} 1110 & 24 \\ \hline 150 & 46 \\ 6 & \end{array} \ , \quad \begin{array}{r|l} 24 & 6 \\ \hline 0 & 4 \end{array}$$

Donc $2244 \wedge 1134 = 6$

Mais l'algorithme fournit "en remontant le calcul" une solution particulière (u,v) de l'équation de Bezout $au + bv = a \wedge b$:

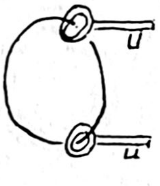
$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) = (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3} = \dots$$

$r_n = a \wedge b$ s'exprime ainsi comme combinaison de r_{n-1} et r_{n-2}, puis de r_{n-2} et r_{n-3}, ... et finalement de a et b. Ainsi dans l'exemple précédent :

$$6 = 1110 - 46.24 = 1110 - 46(1134 - 1.1110) = 47.1110 - 46.1134$$
$$= 47.(2244 - 1.1134) - 46.1134 = \underbrace{47}_{u}.2244 \underbrace{-93}_{v}.1134 .$$

On laisse au lecteur le soin de décrire complètement un algorithme de calcul du pgcd de plusieurs entiers $a_1, \dots, a_p$, et d'une solution particulière de l'équation de Bezout correspondante.

7- On énonce ici le "théorème de Gauss" sous deux formes d'ailleurs équivalentes :



<u>Première forme</u> : $\forall a,b,c \in \mathbb{Z}$; $a | bc$ et $a \wedge b = 1 \Rightarrow a | c$

Preuve : $\exists u,v,w \in \mathbb{Z}$, $au + bv = 1$ et $bc = aw$. D'où $c = acu + bcv = a(cu + vw)$. ∎

<u>Deuxième forme</u> : $\forall a,b,c \in \mathbb{Z}$; $a \wedge b = 1$, $a | c$ et $b | c \Rightarrow ab | c$

Preuve : $\exists u \in \mathbb{Z}$, $c = au$; donc $b | au$ et $a \wedge b = 1$; par la première forme, $b | u$: $\exists v \in \mathbb{Z}$, $u = bv$; donc $c = (ab)v$. ∎

Exemple d'application : montrons que si a, b, n sont des entiers et que n est divisible par a^2 et par b^2, alors n est aussi divisible par ab.
Preuve : posons $d = a \wedge b$. Il existe alors $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$; de plus $a' \wedge b' = 1$. Comme $a^2 = d^2 a'^2$ divise n, il existe n' tel que $n = d^2 n'$. Alors a'^2 et b'^2 divisent n'. Donc $a' | n'$ et $b' | n'$. Comme $a' \wedge b' = 1$, par le théorème de Gauss, $a'b' | n'$; donc $(da')(db') | d^2 n'$, c'est-à-dire $ab | n$. ∎

<u>Remarque</u> : 12 est divisible par 4 et par 6, mais pas par $4 \times 6 = 24$ ($4 \wedge 6 = 2$). Par contre tout entier divisible par 3 et par 8 l'est par $3 \times 8 = 24$, puisque $3 \wedge 8 = 1$.

Une application importante du théorème de Gauss est la <u>résolution complète</u> d'une équation de Bezout : trouver toutes les familles $u_1, \dots, u_p$ d'entiers telles que $a_1u_1 + \dots + a_pu_p = a_1 \wedge \dots \wedge a_p$. On n'explicite ici que le cas le plus simple, celui de deux entiers premiers entre eux, a et b : trouver tous les couples (u,v) tels que $au + bv = 1$ (en supposant $a \wedge b = 1$, sinon il n'y a aucune solution d'après 5). L'algorithme d'Euclide du 6 fournit une première solution (u_0, v_0). Si (u,v) en est une autre, on a $au + bv = 1 = au_0 + bv_0$, d'où $a(u-u_0) = b(v_0 - v)$. Donc $b | a(u-u_0)$, et puisque $a \wedge b = 1$, $b | u - u_0$ (Gauss), soit $u - u_0 = bw$ avec $w \in \mathbb{Z}$; d'où $abw = b(v_0 - v)$, soit (si $b \neq 0$) $v_0 - v = aw$. Finalement : $u = u_0 + wb$ et $v = v_0 - wa$, avec $w \in \mathbb{Z}$. Réciproquement pour tout entier w le couple (u,v) souligné est une solution, puisque $au + bv = au_0 + awb + bv_0 - bwa = au_0 + bv_0 = 1$. ■

8- Si $a_1, \dots, a_p$ sont des entiers, l'intersection $Ia_1 \cap \dots \cap Ia_p$ est encore un idéal, donc de la forme I_m avec $m \in \mathbb{Z}$ (théorème 3). C'est dire que l'ensemble des multiples communs de a_1, de a_2, ..., de a_p n'est autre que l'ensemble des multiples de m. m est donc le <u>plus petit commun multiple</u> (p.p.c.m) de $a_1, \dots, a_p$, au sens que tout autre multiple commun en est un multiple. On le note ici $a_1 \vee \dots \vee a_p$; lui aussi n'est défini qu'au signe près.

Par exemple $4 \vee 6 = 12$; et pour tout $a \in \mathbb{Z}$, $a \vee 0 = 0$ et $a \vee 1 = a$. Il est clair aussi que $a \vee b = b \vee a$ et que $a_1 \vee a_2 \vee \dots \vee a_p = (\dots((a_1 \vee a_2) \vee a_3 \dots) \vee a_p$.

Un algorithme de calcul des ppcm peut donc se déduire de l'algorithme d'Euclide de calcul des pgcd, combiné avec la formule :

$$\forall a,b \in \mathbb{Z}^* \qquad \boxed{a \vee b = \frac{ab}{a \wedge b}}.$$

Preuve de la formule : si $a \wedge b = 1$, $a \vee b = ab$ car tout multiple de a et de b est un multiple de ab d'après le théorème de Gauss. Sinon $a = da'$, $b = db'$ avec $d = a \wedge b$ et $a' \wedge b' = 1$. Comme il est clair que $(da') \wedge (db') = d(a' \wedge b')$ et $(da') \vee (db') = d(a' \vee b')$, il vient $a \vee b = d(a' \vee b') = da'b' = \frac{(da')(db')}{d} = \frac{ab}{a \wedge b}$. ■

Ⓒ <u>DÉCOMPOSITION EN FACTEURS PREMIERS</u>

1- Un entier naturel $p \geq 2$ est appelé <u>nombre premier</u> s'il n'a pas de diviseur non trivial ($q | p \Rightarrow q = \pm 1$ ou $\pm p$). Ainsi 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... sont premiers.

<u>Remarque</u> : pour $p \geq 2$, <u>p premier</u> $\Leftrightarrow \forall n \in \mathbb{Z}$, <u>$p \wedge n = 1$ ou p</u> (car $p \wedge n | p$)

On notera ici $\mathcal{P} \subset \mathbb{N}^*$ l'ensemble des nombres premiers.

<u>Théorème</u> : <u>Tout entier naturel ≥ 2 s'écrit de façon unique (à l'ordre près) comme produit de nombres premiers</u> : $n = p_1 \cdot p_2 \cdot \dots \cdot p_q$ (avec $p_j \in \mathcal{P}$ pour $j = 1, 2, \dots q$)

Une telle écriture s'appelle "décomposition de n en facteurs premiers."

Preuve : L'unicité se montre grâce au théorème de Gauss : si $p_1 \cdots p_q = p'_1 \cdots p'_{q'}$, $p_1 | p'_1 \cdot (p'_2 \cdots p'_{q'})$; si $p_1 \neq p'_1$, $p_1 \wedge p'_1 = 1$, donc $p_1 | p'_2 \cdots p'_{q'}$, et on recommence... Finalement p_1 est l'un des facteurs de droite ; on simplifie et on recommence... (une rédaction correcte ne peut se passer de récurrences !). L'existence d'une telle décomposition se montre aussi par récurrence : supposons-la démontrée pour tout $n' < n$. Si alors n est premier, $n = n$ est la décomposition ; sinon $n = n_1 n_2$ avec $n_1 < n$ et $n_2 < n$, d'où $n_1 = p_1 \cdots p_q$, $n_2 = p'_1 \cdots p'_{q'}$, donc $n = p_1 \cdots p_q \cdot p'_1 \cdots p'_{q'}$. ∎

<u>Corollaire</u> (attribué à <u>Archimède</u>) : <u>L'ensemble $\mathcal{P}$ des nombres premiers est infini</u>

Preuve : supposons que $\{p_1, p_2, \ldots, p_k\}$ soit la liste complète des nombres premiers, et posons $n = p_1 \cdots p_k + 1$. Comme $n \geq 2$, n admet une décomposition en facteurs premiers ; soit q l'un de ces facteurs : c'est l'un des p_j de la liste, donc $q | p_1 \cdots p_k$; comme $q | n$, q divise $n - p_1 \cdots p_k = 1$, ce qui est absurde. ∎

2 - En réordonnant les facteurs premiers d'une décomposition, on voit que <u>tout entier $n \geq 2$ s'écrit de façon unique $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_q^{\alpha_q}$</u>, avec $p_1 < p_2 < \cdots < p_q$, les $p_j \in \mathcal{P}$, et les exposants $\alpha_j \in \mathbb{N}$.

Avec la convention habituelle $p^0 = 1$, on peut même écrire $n = \prod_{p_j \in \mathcal{P}} p_j^{\alpha_j}$, le produit portant sur <u>tous</u> les nombres premiers p_j, mais les exposants α_j étant <u>tous nuls sauf un nombre fini</u>. On aura même alors $1 = \prod_{p_j \in \mathcal{P}} p_j^0$. L'intérêt pratique de ces conventions d'écriture est par exemple que, comme on le vérifiera sans peine :

<u>si $a = \prod p_j^{\alpha_j}$ et $b = \prod p_j^{\beta_j}$, alors $a \wedge b = \prod p_j^{\inf(\alpha_j, \beta_j)}$ et $a \vee b = \prod p_j^{\sup(\alpha_j, \beta_j)}$</u>,

chaque produit portant sur l'ensemble $\mathcal{P}$ de tous les nombres premiers.

3 - Les nombres premiers sont donc en quelque sorte les "atomes" de l'anneau des entiers, et la connaissance de la décomposition en facteurs premiers d'entiers "trivialise" leurs propriétés de division, comme le montrent les formules précédentes. Mais en vérité, on connait <u>mal</u> les nombres premiers ; par exemple on ne dispose d'aucune formule permettant de calculer "le n-ième nombre premier p_n" en fonction de n ; ni d'aucun algorithme de calcul de la décomposition en facteurs premiers d'un entier donné, qui soit beaucoup plus intelligent que d'essayer tous les diviseurs possibles l'un après l'autre. Cette ignorance rend précieuses les méthodes du § B.

Illustrons-la encore de deux exemples :

- On appelle "nombres de Fermat" les entiers de la suite $2^{(2^m)} + 1$ $(m = 0, 1, 2, 3, \ldots)$, c'est-à-dire 3, 5, 17, 257, 65.537, ... Ceux qui sont écrits sont premiers, mais pas les suivants, et il faut aller très loin dans cette suite pour y trouver un autre nombre premier (c'est récemment par de gros calculs sur machine qu'on en a trouvé un, qui a été un temps le plus grand nombre premier connu). Est-ce que cette suite contient une infinité de nombres premiers ? On ne sait pas
- On appelle "paire de nombres premiers" consécutifs, deux nombres premiers qui ne diffèrent que de 2 ; par exemple 3 et 5, 5 et 7, 11 et 13, 17 et 19, ..., 101 et 103, ... Y-a-t-il une infinité de telles paires ? On ne sait pas.

(D) LES ENTIERS "MODULO n"

(C) 1 - On choisit un entier $n \geq 2$. On regroupe alors les entiers en tas, en mettant deux entiers dans le même tas dès que leur différence est un multiple de n. Ainsi le tas qui contient un entier $a \in \mathbb{Z}$ donné, qu'on appelle <u>classe</u> de a et qu'on note $\dot{a}$ est l'ensemble $\dot{a} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\} = \{a+kn \mid k \in \mathbb{Z}\}$.

<u>Chaque tas contient un et un seul entier dans l'intervalle $[0, n-1]$, et il y a donc exactement n tas, qui sont $\dot{0}, \dot{1}, \ldots, \dot{\overline{n-1}}$. Chaque entier appartient à une et une seule de ces n classes.</u>

Preuve : d'abord tout entier $p \in \mathbb{Z}$ appartient à une de ces classes, puisque par division euclidienne $p = nq + r$, avec $0 \leq r < n$, et donc $\dot{p} = \dot{r} \in \{\dot{0}, \dot{1}, \ldots, \dot{\overline{n-1}}\}$.
De plus ces n classes sont deux à deux sans intersection, car si $p \in \dot{r} \cap \dot{r}'$, avec $0 \leq r \leq r' < n$, on a $p = nq + r = nq' + r'$, d'où $0 \leq r' - r = n(q - q') < n$, ce qui implique $q - q' = 0$, puis $r = r'$. ∎

2 - Deux entiers sont dits "égaux modulo n" s'ils sont dans la même classe, donc s'ils diffèrent d'un multiple de n. L'ensemble de ces n classes s'appelle l'ensemble des <u>entiers modulo n</u> et se note $\mathbb{Z}/n\mathbb{Z}$ ou encore $\mathbb{Z}/n$, ou même $\mathbb{Z}_n$. Sur cet ensemble à n éléments on définit deux opérations (une somme et un produit), héritées de celles de $\mathbb{Z}$, en posant : <u>$\dot{a} + \dot{b} = \dot{\overline{a+b}}$</u> et <u>$\dot{a}\dot{b} = \dot{\overline{ab}}$</u>, ce qui a bien un sens puisque
$\dot{a} = \dot{a}'$ et $\dot{b} = \dot{b}' \Rightarrow \dot{\overline{a+b}} = \dot{\overline{a'+b'}}$ et $\dot{\overline{ab}} = \dot{\overline{a'b'}}$.
Ces opérations possèdent les mêmes propriétés d'associativité, commutativité et distributivité que celles de $\mathbb{Z}$, puisqu'il suffit de les vérifier sur des <u>représentants</u> entiers de chaque classe considérée, soit : $(\dot{a} + \dot{b}) + \dot{c} = \dot{a} + (\dot{b} + \dot{c})$; $(\dot{a}\dot{b})\dot{c} = \dot{a}(\dot{b}\dot{c})$; $\dot{a} + \dot{b} = \dot{b} + \dot{a}$; $\dot{a}\dot{b} = \dot{b}\dot{a}$; $(\dot{a} + \dot{b})\dot{c} = \dot{a}\dot{c} + \dot{b}\dot{c}$ (quels que soient $a, b, c \in \mathbb{Z}$).

De plus $\dot{0}$ est l'élément neutre de l'addition : $\dot{0} + \dot{a} = \dot{a}$; chaque classe a une classe "opposée", et $-(\dot{a}) = (\dot{-a})$; enfin $\dot{1}$ est l'élément neutre de la multiplication : $\dot{1}\dot{a} = \dot{a}$ (quel que soit $a \in \mathbb{Z}$).

(C) 3 - <u>Théorème</u>. <u>Les trois assertions suivantes sont équivalentes</u> :

(1) <u>Le produit de deux éléments de $\mathbb{Z}/n$ n'est nul que si l'un est nul.</u>
$\forall \dot{a}, \dot{b} \in \mathbb{Z}/n$, $\dot{a}\dot{b} = \dot{0} \Rightarrow \dot{a} = \dot{0}$ ou $\dot{b} = \dot{0}$

(2) <u>Tout élément non nul de $\mathbb{Z}/n$ est inversible.</u>
$\forall \dot{a} \in (\mathbb{Z}/n)^* \ \exists \dot{b} \in \mathbb{Z}/n$, $\dot{a}\dot{b} = \dot{1}$ $\quad ((\mathbb{Z}/n)^* = \mathbb{Z}/n - \{\dot{0}\})$

(3) <u>n est un nombre premier</u>

Preuve : <u>(1) ⇒ (3)</u> si n n'est pas premier, $n = n_1 n_2$ avec $0 < n_1, n_2 < n$, d'où $\dot{n}_1 \neq \dot{0}$, $\dot{n}_2 \neq \dot{0}$, et pourtant $\dot{n}_1 \dot{n}_2 = \dot{n} = \dot{0}$.

$(2)\Rightarrow(1)$: supposons $\dot a\dot b=\dot 0$ et $\dot a\neq\dot 0$; alors a est inversible : $\exists\, \dot u\in\mathbb{Z}/n$, $\dot a\dot u=\dot 1$; donc $\dot 0=\dot u\dot 0=\dot u\dot a\dot b=\dot 1\dot b=\dot b$.

$(3)\Rightarrow(2)$: Si $a\in\mathbb{Z}$ et $\dot a\neq\dot 0$, a n'est pas divisible par n. Comme n est premier, $a\wedge n=1$; donc il existe des entiers u et v tels que $au+nv=1$. D'où : $\dot 1=\dot a\dot u+\dot n\dot v=\dot a\dot u+\dot 0=\dot a\dot u$, et $\dot u$ est l'inverse de $\dot a$ dans $\mathbb{Z}/n$. ■

Par exemple l'inverse de $\dot 3$ dans $\mathbb{Z}/17$ est $\dot 6$, puisque $2.17-11.3=1$, et que $\dot{\overline{-11}}=\dot 6$ puisque $6-(-11)=17$.

4 - "Problème chinois" : On se donne quatre entiers $p,q\geqslant 2$ et a,b. Trouver tous les entiers x tels que $x\equiv a\ (\mathrm{mod}.\,p)$ et $x\equiv b\ (\mathrm{mod}.\,q)$ (c'est-à-dire $\dot x=\dot a$ dans $\mathbb{Z}/p$, et $\dot x=\dot b$ dans $\mathbb{Z}/q$). On peut généraliser en se donnant plus de deux conditions de ce type.

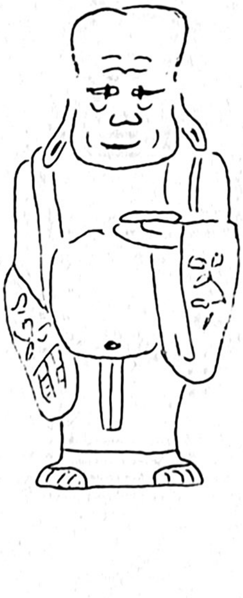
⌜Le nom de "problème chinois" vient de ce que ce type de question est envisagé ... et résolu dans de vieux classiques chinois qui remontent à la dynastie Han, des derniers siècles avant Jésus-Christ.⌟

"Théorème chinois" : Si $p\wedge q=1$, un tel x existe, et est unique à un multiple près de pq arbitraire.

Preuve et méthode de calcul : si $x=a+mp=b+nq$, c'est que $mp-nq=b-a$. L'équation de Bezout $mp-nq=1$ est résoluble puisque $p\wedge q=1$, et l'algorithme d'Euclide fournit une solution particulière (m_0,n_0) : $m_0p-n_0q=1$. Posant $m_1=m_0(b-a)$ et $n_1=n_0(b-a)$, on a donc $m_1p-n_1q=b-a$. Si (m,n) est une autre solution de $mp-nq=b-a$, il vient $(m-m_1)p=(n-n_1)q$, et q divise $m-m_1$ par le théorème de Gauss, soit $m=m_1+qr$ pour un certain $r\in\mathbb{Z}$, et par suite $n=n_1+pr$.

On obtient donc pour chaque $r\in\mathbb{Z}$ une solution du problème en posant $x=a+m_0(b-a)p+rpq=b+n_0(b-a)q+rpq$. On les a toutes ainsi, car si x et x' sont deux solutions, $x-x'$ est un multiple de p et de q, donc de pq (Gauss encore). ■

⌜Exemple : trouver tous les entiers qui valent 5 modulo 7 et 11 modulo 17. (Réponse : ce sont tous ceux de la forme $96+119k$, avec $k\in\mathbb{Z}$).⌟



CHAPITRE 2 : DES ENTIERS AUX COMPLEXES

« J'ai additionné la surface et le coté de mon carré et le tiers du coté de mon carré, soit $\frac{11}{12}$. Tu poseras 1. Tu ajouteras le tiers de 1 à 1 : $1+\frac{1}{3}$. Sa moitié est $\frac{2}{3}$. Tu croiseras $\frac{2}{3}$ et $\frac{2}{3}$: $\frac{4}{9}$. Tu ajouteras à $\frac{11}{12}$: $\frac{49}{36}$; c'est le carré de $\frac{7}{6}$, ou de $1+\frac{1}{6}$. Tu soustrairas les $\frac{2}{3}$ que tu as croisés, de $1+\frac{1}{6}$: $\frac{1}{2}$. C'est le coté du carré. »

(Tablette BM 13.901, de l'Ancien Âge Babylonien ; Problème n° 5 ; dans Thureau-Dangin, "Textes mathématiques babyloniens", Leiden, 1938)

(On aura reconnu l'équation $x^2+\frac{4}{3}x=\frac{11}{12}$, et la formule $x=-\frac{1}{2}\cdot\frac{4}{3}+\sqrt{\left(\frac{1}{2}\cdot\frac{4}{3}\right)^2+1\cdot\frac{11}{12}}$)

(A) JUSQU'À L'ÉQUATION DU SECOND DEGRÉ

1- Que faut-il rajouter à a pour trouver b ? C'est l'équation algébrique de base : $x+a=b$. Posée dans l'ensemble $\mathbb{N}$ des entiers naturels (c'est-à-dire pour $a,b\in\mathbb{N}$, et en cherchant les solutions x dans $\mathbb{N}$), elle n'a déjà de solution que si $a\leq b$. C'est pour pouvoir énoncer « la solution est $x=b-a$ » qu'on a inventé les entiers négatifs ; mais l'anneau $\mathbb{Z}$ de tous les entiers est aussi doté d'une multiplication, qui permet de poser de façon naturelle "l'équation algébrique générale du premier degré" $ax+b=c$.

Posée dans $\mathbb{Z}$, elle n'a bien sûr de solution que si $a|c-b$. Comme la seule solution possible est "un nombre qui, multiplié par a, vaut $c-b$", s'il n'y en a pas dans $\mathbb{Z}$, on l'invente : c'est la "fraction" $\frac{c-b}{a}$. On est ainsi amené, pour résoudre l'équation du premier degré, à fabriquer le "corps des nombres rationnels" $\mathbb{Q}$: on note $\frac{p}{q}$ un nouveau nombre qui est par définition "la" solution de $qx-p=0$ (ceci pour $p,q\in\mathbb{Z}$, et pour $q\neq 0$ seulement ; car $q=0$ impliquerait $qx=0$ pour tout x, donc que l'équation considérée n'a aucune solution si $p\neq 0$, et a tout nombre pour solution si $p=0$).

Mais la solution de $qx-p=0$ l'est aussi de $(rq)x-(rp)=0$, et $\frac{rp}{rq}$ est donc le même nombre que $\frac{p}{q}$ (en particulier $\frac{-p}{-q}=\frac{p}{q}$). De plus, si $q|p$, disons $p=qs$, la solution $x=s$ était déjà dans $\mathbb{Z}$, et il faut identifier $\frac{p}{q}=\frac{qs}{q}$ à s ; par exemple $\frac{p}{1}=p$. On aboutit ainsi à la définition formelle qui suit du corps des nombres rationnels (que l'on ne comprend bien qu'en se souvenant que le rationnel $\frac{p}{q}$ n'est pas autre chose que "quelqu'un qui multiplié par l'entier q vaut l'entier p") :

On considère l'ensemble $\mathbb{Z} \times \mathbb{Z}^*$ des couples d'entiers (p,q) avec $q \neq 0$, et on regroupe ses éléments en <u>classes</u> : (p,q) est dans la même classe que (p',q') si et seulement si $pq' = p'q$, et on note $\frac{p}{q}$ la classe de (p,q) : donc $pq' = p'q \Leftrightarrow \frac{p}{q} = \frac{p'}{q'}$. $\mathbb{Q}$ est l'ensemble des classes. On identifie $\mathbb{Z}$ à une partie de $\mathbb{Q}$ par $p \longleftrightarrow \frac{p}{1}$. Chaque élément de $\mathbb{Q}$ a un <u>représentant</u> unique (p_0, q_0) tel que $p_0 \wedge q_0 = 1$ et $q_0 > 0$, qu'on appelle son <u>expression irréductible</u> ; les autres sont de la forme (rp_0, rq_0) pour tout $r \in \mathbb{Z}^*$. Un rationnel $\frac{p}{q}$ est entier (c'est-à-dire $\in \mathbb{Z}$) si et seulement si $q_0 = 1$.

On prolonge à $\mathbb{Q}$ les opérations de $\mathbb{Z}$ en posant :

$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + qp'}{qq'}$ (forcément, puisque $q'(q \cdot \frac{p}{q}) + q\,(q' \cdot \frac{p'}{q'}) = pq' + qp'$)

et $\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$ (forcément, puisque...)

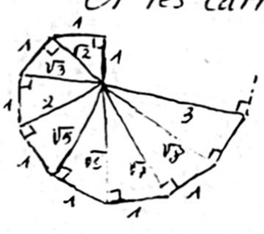
Les entiers 0 et 1 sont éléments neutres respectifs de l'addition et de la multiplication, dont les propriétés d'associativité, commutativité et distributivité sont encore vraies : $\forall r, r', r'' \in \mathbb{Q}$, $r(r'r'') = (rr')r''$ et $r + (r' + r'') = (r + r') + r''$, $r + r' = r' + r$ et $rr' = r'r$, $r(r' + r'') = rr' + rr''$. Enfin tout rationnel $\frac{p}{q}$ a un opposé $-(\frac{p}{q}) = \frac{-p}{q}$, et tout rationnel <u>non nul</u> $\frac{p}{q}$ a un inverse $\frac{q}{p}$.

L'<u>ordre</u> total de $\mathbb{Z}$ se prolonge aussi à $\mathbb{Q}$: $\frac{p}{q} \leq \frac{p'}{q'} \Leftrightarrow pq' \leq p'q$ dès que $qq' > 0$, ce qu'on peut toujours supposer. De même la "valeur absolue"...

2 – Tant qu'on fait de l'algèbre "linéaire", c'est-à-dire quand on considère des équations du <u>premier</u> degré, le corps $\mathbb{Q}$ ainsi construit est suffisant (remarquons toutefois que pour <u>bien</u> calculer avec des nombres rationnels, il faut maîtriser l'arithmétique : pgcd, ppcm, ...). Mais dès qu'on considère l'équation du <u>second</u> degré $ax^2 + bx + c = 0$, on a besoin d'"extraire des racines carrées", et pour cela d'inventer des nombres "<u>irrationnels</u>".

Par exemple l'équation $x^2 - 2 = 0$ n'a aucune solution rationnelle $\frac{p}{q}$ (en effet on peut supposer $p \wedge q = 1$; or $p^2 = 2q^2$ impliquerait p pair, donc $4 | p^2$, d'où $2 | q^2$, et q serait aussi pair ∎).

Or les carrés exigent des diagonales : $\sqrt{2}$ △ 1, 1, et plus généralement le théorème de Pythagore nous force à définir les racines carrées de n'importe quel entier naturel. On plonge donc $\mathbb{Q}$ dans un corps de nombres plus grand.



Cette référence à la géométrie n'est pas innocente : s'il s'agissait seulement de résoudre les équations du second degré, les nombres de la forme $x \pm \sqrt{y}$, avec $x, y \in \mathbb{Q}$, feraient l'affaire, comme on va le voir ; mais d'autres nombres nous supplient d'exister, liés à la géométrie, comme π et e par exemple. Au XIXe siècle, on a eu la main lourde en définissant le corps $\mathbb{R}$ des nombres <u>réels</u>. Comme leur définition et l'étude de leurs propriétés fait l'objet du cours d'<u>analyse</u>, on se contentera ici de quelques remarques, avant de les supposer <u>connus</u>.

Un nombre réel est défini par ses approximations rationnelles, c'est-à-dire par une suite infinie de nombres rationnels $(x_n)_{n\in\mathbb{N}}$, qui est "de Cauchy", c'est-à-dire que chaque chiffre de leur développement décimal se stabilise à partir d'un certain numéro n :

$$\forall N\in\mathbb{N},\ \exists n_0\in\mathbb{N},\ \forall p,q\geqslant n_0,\ |x_p-x_q|<10^{-N}.$$

Par exemple e est défini par la suite $e_n = 1+\frac{1}{1!}+\frac{1}{2!}+\dots+\frac{1}{n!}$,

$\frac{\pi}{2}$ par la suite $\left(\frac{\pi}{2}\right)_n = 1+\frac{1}{2}\cdot\frac{1}{3}+\frac{1.3}{2.4}\cdot\frac{1}{5}+\frac{1.3.5}{2.4.6}\cdot\frac{1}{7}+\dots+\frac{1.3.5\dots(2n-1)}{2.4.6\dots(2n)}\cdot\frac{1}{(2n+1)}$.

La suite (x_n) peut être définie de nombreuses façons, par exemple par un procédé récurrent qui permet de calculer x_n quand on connaît déjà les précédents. Ainsi le développement décimal "à n'importe quel ordre" d'une racine carrée peut se calculer par un algorithme récurrent bien connu, illustré ici pour $\sqrt{2}$:

2,00'00'00'00'00'...	1,41421...
1 00	24×4
400	281×1
11900	2824×4
60400	28282×2
383800	282841×1
100959 ...	...

$\Rightarrow \sqrt{2} = 1,41421\dots$

Mais beaucoup de suites (x_n) différentes peuvent définir le même nombre réel : par exemple $x_n = 1$ et $x'_n = 1+\frac{1}{n}$ définissent toutes les deux le nombre 1 ; ou encore e est aussi défini par la suite $\left(1+\frac{1}{n}\right)^n$. Et une définition formelle d'un nombre réel est une classe de suites de Cauchy de rationnels...

Quoi qu'il en soit on fabrique ainsi un corps $\mathbb{R}$ des nombres réels qui contient $\mathbb{Q}$ (les classes des suites constantes), et auquel on étend toutes les propriétés déjà citées des rationnels : addition et multiplication associatives, commutatives et distributive ; éléments neutres respectifs 0 et 1 ; tout réel x a un opposé $-x$, et tout réel non nul x a un inverse $\frac{1}{x}$; ordre total et valeur absolue positive ; "règle des signes" ;...

3- Pour résoudre alors l'équation du second degré $ax^2+bx+c=0$ (avec $a,b,c\in\mathbb{R}$, $a\neq 0$), on ramène la question à l'extraction d'une racine carrée (et le procédé récurrent ci-dessus marche aussi bien pour calculer la racine d'un réel positif dont on connaît le développement décimal), par une astuce déjà connue des Babyloniens il y a 4000 ans : le premier terme de l'équation pouvant s'écrire aussi

$a\left(x+\frac{b}{2a}\right)^2-\frac{b^2}{4a}+c$, elle équivaut à $\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{(2a)^2}$,

et revient donc à extraire une racine carrée du "discriminant" $\Delta = b^2-4ac$. Si $\Delta\geqslant 0$, il a comme on vient de le voir une racine carrée α, et par suite il en a deux, car $(-\alpha)^2=\alpha^2=\Delta$ (règle des signes). Mais il ne peut en avoir d'autres, car

$0 = x^2 - \Delta = x^2 - \alpha^2 = (x-\alpha)(x+\alpha) \Rightarrow x-\alpha = 0$ ou $x+\alpha=0$
(car le corps des réels est "intègre" : si $a,b \in \mathbb{R}$ et $ab=0$, alors $a=0$ ou $b=0$; puisque si $a \neq 0$, $b = 1.b = (\frac{1}{a}.a)b = \frac{1}{a}(ab) = \frac{1}{a}.0 = 0$ ■)

Donc si $\Delta = b^2-4ac \geqslant 0$, l'équation $ax^2+bx+c=0$ a deux solutions, données par les formules bien connues $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, éventuellement confondues lorsque $\Delta = 0$ (on dit qu'elle a alors la racine "double" $x = -\frac{b}{2a}$, et le polynôme ax^2+bx+c est à un facteur près un "carré parfait" : $ax^2+bx+c \equiv a(x+\frac{b}{2a})^2$.)

Mais l'équation $x^2+1=0$ par exemple n'a pas de solution réelle puisque $x^2 \geqslant 0 \Rightarrow x^2+1 \geqslant 1 > 0$. On fabrique alors un nouveau corps de nombres en rajoutant à $\mathbb{R}$ le nombre "imaginaire" i, qui est par définition une racine carrée de -1, puis tout ce qu'on obtient par somme et par produit, c'est-à-dire toutes les combinaisons de 1 et i à coefficients réels, soit $a+bi$. Formellement, le corps $\mathbb{C}$ des nombres complexes est donc l'ensemble des couples (a,b) de nombres réels, muni des deux opérations :

$$\begin{cases}(a,b)+(c,d) = (a+c, b+d) \\ (a,b).(c,d) = (ac-bd, ad+bc)\end{cases}$$

qui en font un anneau commutatif ; on note i le couple $(0,1)$, a le couple $(a,0)$, ce qui identifie $\mathbb{R}$ à un sous-corps de $\mathbb{C}$; 0 et 1 sont les éléments neutres des deux opérations ; tout nombre complexe $(a,b) = a+bi$ a pour opposé $(-a,-b) = -a-bi$; tout nombre complexe non nul (c'est-à-dire autre que $(0,0)$.) a un inverse $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, soit : $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$ (puisque $(a+bi)(a-bi) = a^2+b^2 \neq 0$).

On prolonge encore à $\mathbb{C}$ la notion de "valeur absolue" en posant : $|a+bi| = \sqrt{a^2+b^2}$, et c'est encore un nombre réel positif, (strictement sauf $|0|=0$), qu'on appelle aussi le "module" du nombre complexe.

b] Mais on n'a plus de relation d'ordre total naturelle dans $\mathbb{C}$.

Enfin deux couples distincts (a,b) et (a',b') ne peuvent définir le même nombre complexe, puisque

$$a+bi = a'+b'i \Leftrightarrow a-a' = (b'-b)i \Rightarrow (a-a')^2 = -(b'-b)^2$$
$$\Leftrightarrow (a-a')^2+(b-b')^2 = 0 \Rightarrow a=a' \text{ et } b=b'. \blacksquare$$

(B) CALCULS DANS LE CORPS DES COMPLEXES

(C) 1 – D'abord tout nombre complexe non nul a deux racines carrées, opposées (donc distinctes !) et pas plus. (On en a qu'une, qui est 0).

Preuve : s'il est réel positif, on le sait ; s'il est réel <0, il s'écrit $-a$, avec $a>0$ et ses racines sont $\pm i\sqrt{a}$ comme on l'a vu ci-dessus. S'il n'est pas réel, il s'écrit $a+ib$ avec $a,b \in \mathbb{R}$, $b \neq 0$, et

$(x+iy)^2=a+ib \iff \begin{cases} x^2-y^2=a \\ 2xy=b \ (b\neq 0 \Rightarrow x\neq 0) \end{cases} \implies \begin{cases} y=\dfrac{b}{2x} \\ x^4-ax^2-\dfrac{b^2}{4}=0 \end{cases}$

et $X=x^2$ est un nombre réel positif, solution de $X^2-aX-\frac{b^2}{4}=0$. Comme $\Delta=a^2+b^2>0$, il vient $X=\frac{a\pm\sqrt{a^2+b^2}}{2}$, d'où $X=\frac{a+\sqrt{a^2+b^2}}{2}>0$, et les deux solutions sont : $x_\pm=\pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}$, $y_\pm=\frac{b}{2x_\pm}$. ■

Considérons alors l'équation du second degré à coefficients complexes $az^2+bz+c=0$ $(a,b,c\in\mathbb{C}, a\neq 0)$. Le même traitement qu'en A-3 la ramène à $\left(x+\frac{b}{2a}\right)^2=\frac{\Delta}{(2a)^2}$, avec $\Delta=b^2-4ac$, et elle est donc résolue par la formule

$$\boxed{x_\pm=\frac{-b\pm\sqrt{b^2-4ac}}{2a}},$$

à condition de bien comprendre que le symbole "$\pm\sqrt{\ }$" utilisé ici signifie "l'une ou l'autre des deux racines carrées opposées du nombre complexe" écrit sous le radical, alors que le sens initial du symbole $\sqrt{\ }$ était la racine carrée ≥ 0 d'un nombre réel ≥ 0 (calculable par exemple par le procédé du A-2).

En particulier l'équation du second degré dans $\mathbb{C}$ a deux solutions, (éventuellement confondues lorsque $\Delta=0$). Si a,b,c sont réels, les deux solutions sont réelles lorsque $\Delta\geq 0$, non réelles lorsque $\Delta<0$.

Exemple : résoudre $(1+2i)x^2-10(1+i)x+5(3+4i)=0$.
Le discriminant "simplifié" a pour racines $\pm(1-2i)$, et les deux solutions sont donc $4-3i$ et $2+i$.

Remarquons enfin ici que deux nombres complexes ont pour somme s et pour produit p si et seulement si ce sont les deux solutions (distinctes ou non) de l'équation du second degré $x^2-sx+p=0$.

Preuve : $\left.\begin{matrix} x_1+x_2=s \\ x_1x_2=p \end{matrix}\right\} \Rightarrow x_1^2-sx_1+p=x_1^2-(x_1+x_2)x_1+x_1x_2=0$ et de même $x_2^2-sx_2+p=0$, tandis que les solutions $\frac{s\pm\sqrt{s^2-4p}}{2}$ de l'équation ont bien pour somme s et pour produit p. ■

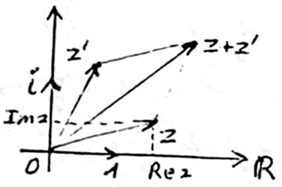
2- L'usage est courant de noter z un nombre complexe. L'écriture $z=a+ib$, avec a et b réels étant unique, on appelle a la partie réelle de z, notée $\operatorname{Re} z$, b sa partie imaginaire, notée $\operatorname{Im} z$, et on appelle complexe conjugué de z le nombre $\bar{z}=a-ib=\operatorname{Re} z-i\operatorname{Im} z$, de sorte que :

$z+\bar{z}=2\operatorname{Re} z\in\mathbb{R}$, $z-\bar{z}=2i\operatorname{Im} z\in i\mathbb{R}$, $z\bar{z}=(\operatorname{Re} z)^2+(\operatorname{Im} z)^2=|z|^2\geq 0$,

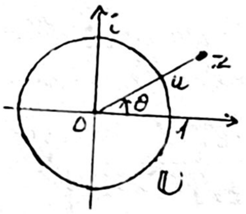
si $z\neq 0$ $\frac{1}{z}=\frac{\bar{z}}{|z|^2}$; en particulier l'inverse d'un nombre complexe de module 1 est son conjugué : $|z|=1 \iff \frac{1}{z}=\bar{z}$.

Si $z,z'\in\mathbb{C}$, on a $\overline{z+z'}=\bar{z}+\bar{z}'$, $\overline{zz'}=\bar{z}\bar{z}'$, $|zz'|=|z||z'|$, et $|z+z'|\leq|z|+|z'|$, d'où encore pour $z\neq 0$, $\left|\frac{1}{z}\right|=\frac{1}{|z|}$ et $|z^n|=|z|^n$ pour tout $n\in\mathbb{Z}$.

3 - Il est commode d'identifier $\mathbb{C}$ à un plan « rapporté à un repère orthonormé » d'origine O et dont les vecteurs de base sont 1 et i. Le nombre z s'identifie alors au point du plan de coordonnées $\operatorname{Re} z$ et $\operatorname{Im} z$, et le sous-corps $\mathbb{R}$ de $\mathbb{C}$ aux points du premier axe. L'addition des complexes se fait alors comme celle des vecteurs du plan, par la "règle du parallélogramme", et le module d'un nombre complexe est sa distance (euclidienne) à l'origine.



L'ensemble $\mathbb{U}$ des nombres complexes de module 1 s'identifie au "cercle-unité" (de centre O et de rayon 1). Il est clair qu'on peut toujours écrire $z = r.u$ avec $r \geq 0$ et $|u| = 1$; et que cette écriture est unique dès que $z \neq 0$ (et alors $r > 0$) : il vient en effet $r = |z|$, puis si $z \neq 0$, $u = \frac{z}{|z|}$. De plus si $u = a + ib$ $(a, b \in \mathbb{R})$, on a $a^2 + b^2 = 1$, et a et b sont donc les cosinus et sinus d'un même angle :



$\exists 1\, \theta \in \mathbb{R}/_{2\pi\mathbb{Z}}$, $u = \operatorname{Cos}\theta + i \operatorname{Sin}\theta$. On appelle θ l'argument de z.

Si $x = \operatorname{Re} z$ et $y = \operatorname{Im} z$, on tire de $z = x + iy = r(\operatorname{Cos}\theta + i\operatorname{Sin}\theta)$:

$r = \sqrt{x^2+y^2}$, $\operatorname{Cos}\theta = \frac{x}{r}$, $\operatorname{Sin}\theta = \frac{y}{r}$, $\operatorname{Tg}\theta = \frac{y}{x}$.

Notons $u_\theta = \operatorname{Cos}\theta + i\operatorname{Sin}\theta$ le nombre complexe de module 1 et d'argument θ.

On a : $u_\theta u_{\theta'} = (\operatorname{Cos}\theta + i\operatorname{Sin}\theta)(\operatorname{Cos}\theta' + i\operatorname{Sin}\theta') = (\operatorname{Cos}\theta\operatorname{Cos}\theta' - \operatorname{Sin}\theta\operatorname{Sin}\theta') + i(\operatorname{Sin}\theta\operatorname{Cos}\theta' + \operatorname{Sin}\theta'\operatorname{Cos}\theta)$

$= \operatorname{Cos}(\theta+\theta') + i\operatorname{Sin}(\theta+\theta') = u_{\theta+\theta'}$.

D'où une application surjective $\begin{array}{l}\mathbb{R} \longrightarrow \mathbb{U} \\ \theta \longmapsto u_\theta\end{array}$ qui envoie 0 (et tous les multiples entiers de 2π) sur 1, la somme sur le produit, et donc l'opposé sur l'inverse : $u_{-\theta} = \frac{1}{u_\theta}$. On l'appelle exponentielle imaginaire et on la note $u_\theta = e^{i\theta}$. On a donc par définition :

$e^{i\theta} . e^{i\theta'} = e^{i(\theta+\theta')}$, $e^{-i\theta} = \frac{1}{e^{i\theta}} = \overline{e^{i\theta}}$, et $\forall k \in \mathbb{Z}$, $e^{2ik\pi} = 1$.

Si $z, z' \in \mathbb{C}^*$, $|z| = r$, $|z'| = r'$, $\theta = \arg z$, $\theta' = \arg z'$, il vient

$zz' = re^{i\theta} r' e^{i\theta'} = (rr') e^{i(\theta+\theta')}$, d'où : $\begin{cases} |zz'| = rr' = |z||z'| \\ \arg(zz') = \theta + \theta' = \arg z + \arg z' \end{cases}$

Les modules se multiplient, les arguments s'ajoutent, et la multiplication d'un nombre complexe par un autre, de module r et d'argument θ, s'interprète donc géométriquement comme la similitude directe de rapport r et d'angle θ.

4 - On définit plus généralement l'exponentielle complexe comme l'application surjective de $\mathbb{C}$ sur $\mathbb{C}^*$, notée $z \longmapsto e^z$, définie par

$\boxed{e^z = e^{\operatorname{Re} z}(\operatorname{Cos}(\operatorname{Im} z) + i\operatorname{Sin}(\operatorname{Im} z))}$, autrement dit si $z = x + iy$,

$e^z = e^x(\operatorname{Cos} y + i \operatorname{Sin} y)$, donc $x = \operatorname{Log}|e^z|$ et $y = \arg e^z$.

On a $e^{z+z'} = e^z e^{z'}$, $e^0 = 1$, $e^{-z} = \frac{1}{e^z}$, $e^{\bar z} = \overline{e^z}$, $(e^z)^n = e^{nz}$ $(n \in \mathbb{Z})$,

$e^z > 0$ pour $z \in \mathbb{R}$, et $e^z = 1 \Leftrightarrow z \in 2i\pi\mathbb{Z}$.

Par exemple, on a la fameuse "Formule d'Euler" $\boxed{e^{i\pi}+1=0}$, de même que $e^{i\frac{\pi}{2}}=i$, $e^{\frac{3i\pi}{2}}=-i$, $\sqrt{2}\,e^{i\frac{\pi}{4}}=1+i$, ...

Comme $\operatorname{Cos} n\theta + i \operatorname{Sin}\theta = e^{in\theta} = (e^{i\theta})^n = (\operatorname{Cos}\theta + i\operatorname{Sin}\theta)^n$ ("formule de Moivre"), en développant à droite par la formule du binôme et séparant les parties réelle et imaginaire, on obtient

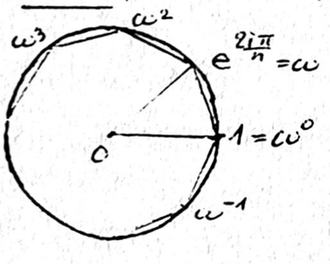
(rappelons la notation $C_n^p = \binom{n}{p} = \dfrac{n!}{p!\,(n-p)!} = \dfrac{n(n-1)\dots(n-p+1)}{1\cdot 2\cdot\dots\cdot p}$, et les formules $C_n^p = C_n^{n-p}$ et $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$, pour $n, p \in \mathbb{N}$, $p \leq n$):

$$\begin{cases} \operatorname{Cos} n\theta = \operatorname{Cos}^n\theta - C_n^2 \operatorname{Cos}^{n-2}\theta \operatorname{Sin}^2\theta + C_n^4 \operatorname{Cos}^{n-4}\theta \operatorname{Sin}^4\theta \dots \\ \operatorname{Sin} n\theta = C_n^1 \operatorname{Cos}^{n-1}\theta \operatorname{Sin}\theta - C_n^3 \operatorname{Cos}^{n-3}\theta \operatorname{Sin}^3\theta + C_n^5 \operatorname{Cos}^{n-5}\theta \operatorname{Sin}^5\theta \dots \end{cases}$$

formules qui permettent de calculer $\operatorname{Cos} n\theta$ et $\dfrac{\operatorname{Sin} n\theta}{\operatorname{Sin}\theta}$ comme polynômes de $c = \operatorname{Cos}\theta$, et d'autres calculs semblables

⟦ Exemples: démontrer que $\operatorname{Cos} 7\theta = 58c^7 - 112c^5 + 5c^3 - 7c$; calculer $\operatorname{Tg} 5x$ en fonction seulement de $t = \operatorname{Tg} x$; ... ⟧

5 - On a vu au début de ce paragraphe que tout nombre complexe a deux racines carrées. Cherchons ses racines n-ièmes. Si $z = \rho e^{i\varphi}$ est solution de l'équation $z^n = r e^{i\theta}$, il vient $\rho^n e^{in\varphi} = r e^{i\theta}$, d'où $\rho = \sqrt[n]{r}$ et $\varphi = \frac{\theta}{n} + \frac{2k\pi}{n}$ $(0 \leq k \leq n-1)$. Le nombre $re^{i\theta}$ (avec $r \neq 0$) a donc exactement n racines n-ièmes de l'unité, qui sont les nombres $z_k = (\sqrt[n]{r}\,.\,e^{i\frac{\theta}{n}})\,.\,e^{\frac{2ik\pi}{n}}$, pour $k = 0, 1, 2, \dots, n-1$; autrement dit les produits de l'une d'entre elles, $z_0 = \sqrt[n]{r}\,e^{i\frac{\theta}{n}}$, par les racines n-ièmes de l'unité, les $e^{\frac{2ik\pi}{n}}$ $(k = 0, 1, \dots, n-1)$, obtenues pour $r = 1$ et $\theta = 0$.



Celles-ci sont les puissances $e^{\frac{2ik\pi}{n}} = \omega^k$, pour $k = 0, 1, \dots, n-1$, de l'une d'entre elles, $\omega = e^{\frac{2i\pi}{n}}$. Leurs images dans le plan sont les sommets d'un polygône régulier à n cotés inscrit au cercle-unité et de sommet $1 = \omega^0$. Il s'ensuit (par similitude) que la figure formée dans le plan par les racines n-ièmes d'un nombre complexe est toujours un polygône régulier centré à l'origine.

Si n est impair, la seule racine n-ième de 1 qui soit réelle est 1, et les autres sont 2 à 2 complexes conjuguées: $\omega^{n-k} = \omega^{-k} = \overline{\omega^k}$

Si n est pair, $-1 = \omega^{\frac{n}{2}}$ est une deuxième racine n-ième réelle de 1.

Notons ici les factorisations du polynôme $X^n - 1$, appelées "identités remarquables":

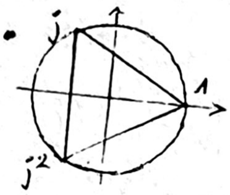
$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \dots + X + 1)$$

$$X^{2p} - 1 = (X-1)(X+1)(X^{2p-2} + X^{2p-4} + \dots + X^2 + 1)$$

et $$X^{2p+1} + 1 = (X+1)(X^{2p} - X^{2p-1} + X^{2p-2} - \dots + 1)$$

6 – Cherchons, à titre d'exemple, les racines n-ièmes de 1 pour $n = 1,2,3,4,5,6,7$.

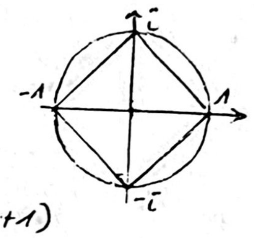
• $x - 1 = 0$ a la seule racine 1, et $x^2 - 1 = 0$ les seules racines 1 et -1.

• 

$x^3 - 1 = (x-1)(x^2+x+1)$ a les trois racines 1, $j = e^{\frac{2i\pi}{3}}$, et $j^2 = e^{\frac{4i\pi}{3}} = e^{-\frac{2i\pi}{3}} = \bar{j} = \frac{1}{j}$, d'où

$x^3 - 1 = (x-1)(x-j)(x-j^2)$, puisque $j + j^2 = 2\,\mathrm{Re}\, j = -1$, et $j \cdot j^2 = j^3 = 1$

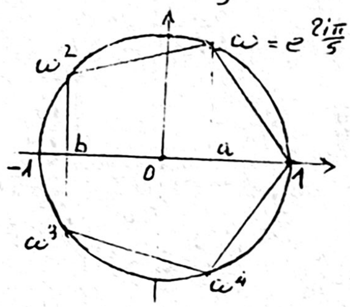
• $x^4 - 1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x-i)(x+i)$, qui a bien pour racines $1, i, -1$, et $-i$, c'est-à-dire les $e^{\frac{2i\pi k}{4}}$, pour $k = 0,1,2,3$.



• Posons maintenant $\omega = e^{\frac{2i\pi}{5}}$ et calculons

$(x-\omega^0)(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4) = (x-1)(x^2-2ax+1)(x^2-2bx+1)$

avec $a = \cos\frac{2\pi}{5}$, $b = \cos\frac{4\pi}{5}$. $\quad = (x-1)\left[x^4 - 2(a+b)x^3 + (2+4ab)x^2 - 2(a+b)x + 1\right]$



Comme on a vérifié dans tous les cas précédents que

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \omega^k), \text{ avec } \omega = e^{\frac{2i\pi}{n}}$$

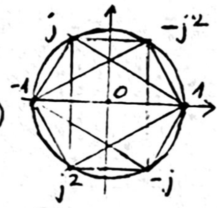
il est tentant de l'admettre ici pour $n = 5$, et d'identifier le polynôme ci-dessus, coefficient par coefficient, à $x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$, ce qui donne $a + b = -\frac{1}{2}$ et $ab = -\frac{1}{4}$, d'où a et b solutions de

$X^2 + \frac{X}{2} - \frac{1}{4} = 0$, et puisque $-1 < b < 0 < a < 1$, $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$ $(\simeq 0{,}309\ldots)$

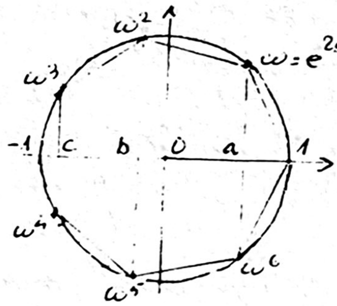
et $\cos\frac{4\pi}{5} = \frac{-\sqrt{5}-1}{4}$ $(\simeq -0{,}809\ldots)$. Ce calcul sera entièrement justifié en 6-A-3.

• De même $x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$

$= (x-1)(x-j)(x-j^2)(x+1)(x+j)(x+j^2) = \prod_{k=0}^{5}\left(x - e^{\frac{2i\pi k}{5}}\right)$



• Enfin admettons de même que $\prod_{k=0}^{6}(x-\omega^k) = (x-1)(x-\omega)(x-\omega^6)(x-\omega^2)(x-\omega^5)(x-\omega^3)(x-\omega^4)$



$= (x-1)(x^2-2ax+1)(x^2-2bx+1)(x^2-2cx+1)$

avec $a = \cos\frac{2\pi}{7}$, $b = \cos\frac{4\pi}{7}$, $c = \cos\frac{6\pi}{7}$,

s'identifie, coefficient par coefficient, à $(x^7-1) = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$; il vient, en développant le premier, le système $\begin{cases} a+b+c = -\frac{1}{2} \\ ab+bc+ca = -\frac{1}{2} \\ abc = \frac{1}{8} \end{cases}$

qui équivaut à dire, comme on le verra en 6-C-1, que a, b, c sont les racines de l'équation du troisième degré

$X^3 + \frac{1}{2}X^2 - \frac{1}{2}X - \frac{1}{8} = 0$, que l'on distinguera en remarquant que $-1 < c < b < 0 < a < 1$

Encore faut-il, pour achever le calcul de $\cos\frac{2\pi}{7}$, savoir résoudre une équation du troisième degré.

7 – Alors que l'équation du second degré est résolue depuis "la plus haute antiquité", c'est à des italiens de la Renaissance qu'on doit les formules de résolution "par radicaux" des équations du troisième et du quatrième degré. (Remarquons qu'à cette époque ni $\mathbb{R}$ ni $\mathbb{C}$ n'étaient encore inventés, et qu'on calculait volontiers avec des nombres mal définis.)

L'équation du troisième degré, $ax^3+bx^2+cx+d=0$, avec $a,b,c,d\in\mathbb{C}$ et $a\neq 0$, peut d'abord se simplifier en divisant tous les coefficients par a, puis lorsque $a=1$, comme $x^3+bx^2+cx+d=(x+\frac{b}{3})^3+(c-\frac{b^2}{3})(x+\frac{b}{a})+d-\frac{bc}{3}+\frac{2b^3}{27}$, par le changement d'inconnue $x'=x+\frac{b}{3}$, on est ramené à résoudre une équation "réduite" (*) $x^3+px+q=0$, avec $p,q\in\mathbb{C}$.

L'idée géniale (due semble-t-il à Scipione del Ferro) est alors de chercher deux nombres u et v tels que $u+v=x$ soit solution de (*), et que $uv=-\frac{p}{3}$: comme $(u+v)^3+p(u+v)+q=u^3+v^3+(3uv+p)(u+v)+q$, ces conditions s'écrivent $\begin{cases}uv=-\frac{p}{3}\\ u^3+v^3=-q\end{cases}$, et impliquent, en posant $U=u^3$, $V=v^3$,
$\begin{cases}U+V=-q\\ UV=-\frac{p^3}{27}\end{cases}$. Donc U et V sont les racines de l'équation du second degré $T^2+qT-\frac{p^3}{27}=0$, et les nombres u et v en sont des racines cubiques ; pour chacune on a donc trois choix possibles, mais il faut encore les coupler de façon que $uv=-\frac{p}{3}$, ce qui est possible puisque $u^3v^3=\frac{-p^3}{27}$. Si (u,v) est un couple admissible, (ju, j^2v) et (j^2u, jv) sont les deux autres, et on obtient ainsi les trois racines complexes (distinctes ou non) de l'équation réduite du troisième degré : $u+v$, $ju+j^2v$, et j^2u+jv, symbolisées par les fameuses "formules de Cardan" :

$$\boxed{x=\sqrt[3]{-\frac{q}{2}+\sqrt[2]{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt[2]{\frac{q^2}{4}+\frac{p^3}{27}}}}$$

qui sont à interpréter avec précaution, mais n'en ramènent pas moins la résolution de l'équation du troisième degré à l'extraction de racines carrées et cubiques. On dit que « l'équation du troisième degré est résoluble par radicaux. »

⌈ Que l'intérêt de cette formule soit plus théorique que pratique, on peut s'en convaincre en tentant de l'employer pour calculer les racines de l'équation $x^3-21x+20=0$ par exemple, qui sont pourtant les entiers 1, 4, et −5. ⌋

En particulier une équation du troisième degré a au plus trois racines.

Indiquons brièvement comment résoudre "par radicaux" l'équation du quatrième degré (procédé dû à Ferrari, élève de Cardan). On commence par la mettre aussi sous forme "réduite" $x^4+ax^2+bx+c=0$ par les mêmes procédés, puis on cherche à factoriser ce polynôme en $(x^2+\xi x+\eta)(x^2-\xi x+\zeta)$, ce qui, en développant et identifiant, donne $\begin{cases}\eta+\zeta=a+\xi^2\\ \xi(\eta-\zeta)=b\\ \eta\zeta=c\end{cases}$.

$\xi=0$ n'est possible que si $b=0$, et, l'équation $x^4+ax^2+c=0$ étant facile à résoudre (d'abord à l'inconnue x^2), on peut supposer $\xi\neq 0$, et le système

écrit équivaut alors à $\begin{cases} 2\eta = a + \xi^2 + \dfrac{b}{\xi} \\ 2\xi = a + \xi^2 - \dfrac{b}{\xi} \\ 4\eta\xi = 4c \end{cases}$, d'où $(a+\xi^2)^2 - \dfrac{b^2}{4\xi^2} = 4c$,

et ξ est solution de l'équation $\xi^6 + 2a\,\xi^4 + (a^2-4c)\,\xi^2 - b^2 = 0$, qui n'est que du troisième degré à l'inconnue $\Xi = \xi^2$, donc résoluble par les formules de Cardan... on trouve, à la fin du calcul, quatre solutions admissibles.

8- Les matheux ont alors cherché des astuces de même type pour résoudre "par radicaux" les équations algébriques de degré plus élevé, vainement pendant trois siècles. C'est vers 1830 que Abel pour l'équation de degré 5, puis Galois pour toutes les autres, ont démontré que c'est impossible : il n'existe pas de formule avec des $\sqrt[n]{\ }$ et des expressions algébriques qui donne les racines de l'équation "générique" de degré ≥ 5, c'est-à-dire valable quels que soient les coefficients de l'équation. Cela n'exclut pas qu'on sache résoudre des équations particulières. Par exemple un équation du type
$ax^6 + bx^5 + cx^4 + dx^3 + cx^2 + bx + a = 0$ se résout facilement en posant $x + \frac{1}{x} = X$, puisqu'elle s'écrit alors (on suppose $a \neq 0$, d'où $x \neq 0$) :
$a(X^3 - 3X) + b(X^2 - 2) + cX + d = 0$ ...

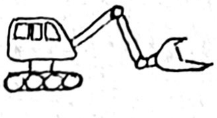
Par contre l'absence de toute formule générale de résolution fait qu'au-delà du degré 4, on ne sait plus énoncer qu'une équation de degré p a au plus p solutions ; à vrai dire on ne sait même pas pour l'instant si elle en a. La réponse est fournie par le théorème suivant, dû à d'Alembert et Gauss et souvent appelé "théorème fondamental de l'algèbre", à juste titre.

9- Théorème fondamental (d'Alembert, Gauss) : Soit P un polynôme à coefficients complexes, de degré $p > 0$. Alors l'équation $P(x) = 0$ a au moins une racine complexe.

Il n'est pas d'usage en Deug de donner une preuve de ce théorème, que nous admettons donc ici. Comme on va l'utiliser souvent, c'est assez choquant, et demande quelques commentaires :

- il serait possible de fournir ici une preuve élémentaire, mais très longue, inspirée de celle de d'Alembert et Gauss, et dont on peut résumer les idées ainsi : par des manipulations algébriques du même type que celles des numéros précédents mais bien plus compliquées, on parvient à associer à P un polynôme Q à coefficients réels et de degré impair, de telle sorte que si Q admet une racine, alors P aussi.

  L'étude de la fonction $x \mapsto Q(x)$ de $\mathbb{R}$ dans $\mathbb{R}$ montre alors que Q admet au moins une racine réelle (Q tend vers $+\infty$ d'un coté, $-\infty$ de l'autre, et une fonction continue ne peut changer de signe sans s'annuler !), d'où le résultat. Ainsi, la preuve du "théorème fondamental de l'algèbre" repose sur un argument d'analyse !
- il existe aujourd'hui d'autres preuves beaucoup plus rapides, qui font appel à la théorie des fonctions holomorphes (toujours de l'analyse, donc), et qu'on expose en cours de licence de maths ; ce qui explique qu'on l'admette jusque là.
- aucune de ces preuves ne fournit d'algorithme de calcul approché des racines ; il en existe pourtant, qui sont difficiles à mettre au point.
- on utilisera souvent ce résultat, aux chapitres 5 et 6, et on en déduira alors aisément que l'équation algébrique de degré p a au plus p racines.



(autre exemple de machine à extraire)

CHAPITRE 3 : GROUPES, ANNEAUX, CORPS

"Les mathématiques sont l'art d'appeler différentes choses du même nom"
(Henri Poincaré, 1854/1912)

(A) GROUPES

1 - Ce chapitre n'est placé ici que pour définir proprement quelques mots nouveaux qui nous ont déjà échappé parfois (comme anneau, corps, intègre, classe), et qu'on entend utiliser librement dans la suite. On reviendra sur certaines de ces notions dans la quatrième partie.

On appelle groupe un ensemble G muni d'une opération, souvent notée comme une multiplication, c'est-à-dire d'une application de $G\times G$ dans G, qui à tout couple (x,y) d'éléments de G associe un élément $x.y$ de G, et qui vérifie les trois propriétés suivantes:

① elle est associative: $\forall x,y,z \in G$, $x(yz)=(xy)z$ (on écrit alors xyz)

② elle admet un élément neutre, noté e: $\exists e \in G$, $\forall x \in G$, $e.x = x.e = x$
(il est alors unique, car si e_1 et e_2 sont neutres, $e_1 = e_1 . e_2 = e_2$)

③ tout élément a un symétrique: $\forall x \in G\ \exists y \in G$, $xy = yx = e$
(le symétrique de $x \in G$ est unique: $y_1 = y_1(xy_2) = (y_1 x) y_2 = y_2$)

Lorsqu'on emploie "la notation multiplicative", c'est-à-dire qu'on écrit l'opération comme un produit, on appelle unité l'élément neutre et on le note 1, et inverse de x son symétrique et on le note x^{-1}, ce qui est justifié par les remarques que $(x^{-1})^{-1} = x$, et $(x^n)^{-1} = (x^{-1})^n$, noté x^{-n}.

2 - Par exemple l'ensemble des nombres complexes de module 1, muni de la multiplication connue, est un groupe, noté $(\mathbb{U},\times)$. De même $(\mathbb{R}^{+*},\times)$, où $\mathbb{R}^{+*}$ est l'ensemble des nombres réels >0.

Autre exemple: soit X un ensemble quelconque et G l'ensemble des bijections de X (applications bijectives de X dans X). Muni de la composition des applications, notée $\circ$, G est un groupe, noté $\mathfrak{S}_X$: la composition d'applications est en effet toujours associative, le neutre est l'application identique $id_X : x \mapsto x$, et l'inverse de la bijection $f : X \to X$ est l'application réciproque.

3 - Si en plus des propriétés ①②③ l'opération du groupe vérifie aussi

④ elle est commutative: $\forall x,y \in G$, $xy = yx$,

on dit que le groupe G est abélien (ou commutatif)

Par exemple $(\mathbb{U},\times)$ et $(\mathbb{R}^{+*},\times)$ sont des groupes abéliens; mais $\mathfrak{S}_X$ ne l'est jamais, dès que l'ensemble X a plus de 2 éléments.

Preuve: Soient x_1, x_2, x_3 trois éléments de X, et f et g les bijections de X telles que
$$\begin{cases} f(x_1)=x_2,\ f(x_2)=x_1,\ f(x_3)=x_3 \text{ et } \forall x \in X-\{x_1,x_2,x_3\},\ f(x)=x \\ g(x_1)=x_1,\ g(x_2)=x_3,\ g(x_3)=x_2 \text{ et } \forall x \in X-\{x_1,x_2,x_3\},\ g(x)=x \end{cases}$$
Alors $f\circ g(x_1) = x_2 \neq x_3 = g\circ f(x_1)$. ■

Lorsqu'un groupe est abélien, on se permet souvent de noter son opération comme une somme ("notation additive"): $(x,y) \mapsto x+y$.

L'élément neutre est alors appelé <u>zéro</u> et noté 0, et le symétrique d'un élément x est appelé son <u>opposé</u> et noté $-x$. Les axiomes ① à ④ se récrivent alors : ① $\forall x,y,z \in G,\ (x+y)+z = x+(y+z)$ (noté $x+y+z$)

② $\exists 0 \in G, \forall x \in G,\ 0+x = x+0 = x$

③ $\forall x \in G, \exists (-x) \in G,\ x+(-x) = (-x)+x = 0$

④ $\forall x,y \in G \quad x+y = y+x$.

Le ① permet d'ôter les parenthèses, et $x+(-y)$ s'écrit $x-y$.

Par exemple $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes abéliens, déjà notés additivement.

4 - Dans un groupe, "<u>on peut toujours simplifier</u>" une équation, c'est-à-dire que $\forall x,y,z \in G$, $xy = xz \Leftrightarrow y = z$ (en effet $y = x^{-1}xy = x^{-1}xz = z$)
De même en notation additive, $x+y = x+z \Leftrightarrow y = z$.
5] Mais si le groupe n'est pas commutatif, $xy = zx \not\Rightarrow y = z$
(Par exemple si $X = \{x_1, x_2, x_3\}$ et $G = \mathfrak{S}_X$, avec les notations f et g du 3, et posant $h = f \circ g \circ f$, on a $f \circ h = g \circ f$, car $f \circ f = f^2 = id_X$, mais $h \neq g$, puisque $f \circ g \neq g \circ f$. ■)

Ⓑ <u>ANNEAUX ET CORPS</u>

1 - On appelle <u>anneau</u> un ensemble A muni de <u>deux</u> opérations,
- une "<u>somme</u>", pour laquelle A est un groupe abélien noté additivement (c'est-à-dire vérifiant les axiomes ① à ④ ci-dessus)
- un "<u>produit</u>", noté multiplicativement et satisfaisant aux deux axiomes suivants :

⑤ le produit est <u>associatif</u> : $\forall x,y,z \in A,\ (xy)z = x(yz)$

⑥ il est <u>distributif</u> par rapport à la somme :
$\forall x,y,z \in A. \quad x(y+z) = xy + xz \quad$ et $\quad (x+y)z = xz + yz$

Introduisons de plus les trois propriétés suivantes :

⑦ la multiplication a un élément <u>neutre</u> : $\exists 1 \in A, \forall x \in A,\ 1.x = x.1 = x$

⑧ tout élément <u>non nul</u> de A est <u>inversible</u> : $\forall x \in A, x \neq 0, \exists x^{-1} \in A, x.x^{-1} = x^{-1}.x = 1$

⑨ le produit est <u>commutatif</u> : $\forall x,y \in A,\ xy = yx$.

Un anneau est dit <u>unitaire</u> si ⑦ est vrai, <u>commutatif</u> si ⑨ est vrai ; Un anneau qui vérifie ⑦ et ⑧ est appelé un <u>corps</u>. Un <u>corps commutatif</u> est un anneau qui vérifie ⑦, ⑧ et ⑨.

<u>Exemples</u> : parmi les ensembles de nombres des chapitres précédents, tous munis des opérations $+$ et $\times$ usuelles, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs, $\mathbb{Z}$ est seulement un anneau commutatif unitaire (seuls 1 et -1 sont inversibles), $\mathbb{N}$ n'est rien du tout, pas même un groupe.

2 - <u>Remarques</u> : • Il résulte des axiomes que dans tout anneau <u>$0.x = x.0 = 0$</u> pour tout x, puisque $x^2 + 0 = x^2 = (x+0).x = x^2 + 0.x$, d'où $0 = 0.x$ ...

• 0 n'est <u>jamais</u> inversible (« <u>diviser par 0 n'a pas de sens</u> »), car le contraire impliquerait : $\forall x,y \in A,\ 0.x = 0 = 0.y$, d'où $x = y$; autrement dit A n'aurait qu'un seul élément, le zéro.

- de même aux axiomes d'un anneau unitaire, on rajoutera le plus souvent
(10) $\underline{1 \neq 0}$; sinon $\forall x \in A$, $x = 1.x = 0.x = 0$, et de nouveau $A = \{0\}$.

- dans tout corps on a la propriété
(*) $\forall x, y$, $\underline{xy = 0 \Rightarrow x = 0 \text{ ou } y = 0}$
puisque $xy = 0$ et $x \neq 0$ implique $y = x^{-1}xy = x^{-1}.0 = 0$.
Un anneau, même non unitaire, qui vérifie (*) est dit __intègre__
Tout corps est donc intègre, mais par exemple $\mathbb{Z}$ aussi est intègre.

- Au § 1-D, on a muni l'ensemble $\mathbb{Z}/n$, pour $n \in \mathbb{N}^*$ d'une structure d'anneau commutatif unitaire, qui a n éléments, et le théorème 1-D-3 peut maintenant s'énoncer :
$\underline{\mathbb{Z}/n \text{ intègre} \Leftrightarrow \mathbb{Z}/n \text{ est un corps} \Leftrightarrow n \text{ est premier}}$

- Les éléments d'un corps sont souvent appelés "nombres", ou "scalaires", ou "constantes", suivant le contexte. Tous les corps qu'on considèrera ici sont commutatifs. On ne mentionnera qu'en exercice un corps non commutatif utile, celui des "quaternions".

3 - Soit K un corps (donc $1 \neq 0$). L'élément de K $\underbrace{1+1+\dots+1}_{p \text{ fois}}$ sera noté $p.1$, ou encore p, comme un entier. Alors :
- ou bien il n'existe pas d'entier $n \in \mathbb{N}^*$ tel que $n.1 = 0$, et on dit que K est __de caractéristique nulle__ (on écrit carac $K = 0$). Dans ce cas, $n.1 \neq n'.1$ dès que $n \neq n'$, même pour $n \in \mathbb{Z}$, en posant $(-p)1 = -(p.1) = \underbrace{-1-1-\dots-1}_{p \text{ fois}}$, et K contient le __sous-anneau__ $\{n.1 \mid n \in \mathbb{Z}\}$ qui est __isomorphe__ à $\mathbb{Z}$ (c'est-à-dire qui s'identifie à $\mathbb{Z}$ avec ses opérations, par $n \longleftrightarrow n.1$)
Comme K est un corps, avec $q \in \mathbb{Z}^*$ il contient aussi son inverse $\frac{1}{q}$, puis $p.\frac{1}{q} = \frac{p}{q}$ pour tout $p \in \mathbb{Z}$, et finalement tout un __sous-corps__ isomorphe à $\mathbb{Q}$. En particulier K est infini.
- ou bien $\{n \in \mathbb{N}^* \mid n.1 = 0\}$ est non vide, et dans ce cas son plus petit élément p est un nombre premier, car $p \geq 2$ puisque $1 \neq 0$, et si $p = p_1p_2$ avec $1 < p_1 \leq p_2 < p$, on aurait $p_1.1 \neq 0$, $p_2.1 \neq 0$, et donc
$(p_1.1)(p_2.1) = \underbrace{(1+1+\dots+1)}_{p_1 \text{ fois}}\underbrace{(1+1+\dots+1)}_{p_2 \text{ fois}} = \underbrace{1+1+\dots+1}_{p_1p_2 \text{ fois}} = p_1p_2.1 = p.1 = 0$,
ce qui contredirait l'intégrité de K.
On dit alors que K est __de caractéristique p__ (on écrit carac $K = p$), et K contient alors le __sous-corps__ $\{0, 1, 2.1, \dots, (p-1).1\}$ __isomorphe__ à $\mathbb{Z}/p$.

4 - Soit K un corps fini. D'après 3 il est de caractéristique p pour un certain p premier, et les multiples de 1 forment un sous-corps de K isomorphe à $\mathbb{Z}/p$. K est donc un espace vectoriel sur $\mathbb{Z}/p$ (cf. chap. 9), de dimension d finie puisqu'il est fini. Il s'ensuit que le nombre d'éléments $\#K$ du corps K est p^d. Réciproquement, pour tout nombre premier p et tout entier d, on sait construire un corps commutatif qui a p^d éléments, et démontrer que deux corps à p^d éléments sont isomorphes. On en déduit alors le "théorème de Wedderburn" : __tout corps fini est commutatif__, que l'on ne sait pas démontrer de façon plus élémentaire. ⫫

—

© EQUIVALENCES, PARTITIONS, ENSEMBLES-QUOTIENTS

1- Une partition d'un ensemble E est la donnée d'une famille de parties de E, $(F_i)_{i\in I}$, telle que $\forall i,j \in I, i\neq j \Rightarrow F_i \cap F_j = \emptyset$; et $\bigcup_{i\in I} F_i = E$.

Chaque élément x de E appartient donc à une et une seule des parties F_i, qu'on appelle <u>classes</u> de la partition ; celle qui contient x s'appelle <u>classe de x</u> et se note $\dot{x}$. Ainsi $\dot{x}$ est l'un des F_i : c'est l'ensemble de tous les éléments de E qui sont dans la même classe que x : $\dot{x} = \{y \in E \mid \dot{y} = \dot{x}\}$

2- A la donnée d'une partition de E on peut associer une "relation binaire" définie sur les couples d'éléments de E : deux éléments $x, y \in E$ sont dits en relation, ce qu'on note $x \mathcal{R} y$ si et seulement si $y \in \dot{x}$, ou encore si $\dot{y} = \dot{x}$. Cette relation est clairement : – <u>réflexive</u> : $\forall x \in E, x \mathcal{R} x$
– <u>symétrique</u> : $\forall x, y \in E, x \mathcal{R} y \Rightarrow y \mathcal{R} x$
– <u>transitive</u> : $\forall x, y, z \in E, x \mathcal{R} y$ et $y \mathcal{R} z \Rightarrow x \mathcal{R} z$

Une relation qui a ces trois propriétés s'appelle une <u>relation d'équivalence</u>, ou encore une <u>équivalence</u> ; elle se note alors souvent $x \sim y$ (ce qui se lit « x équivaut à y ».)

Réciproquement, la donnée d'une relation d'équivalence dans un ensemble E définit une partition de E : on pose, pour tout $x \in E$, $\dot{x} = \{y \in E \mid y \sim x\}$. Comme $x \sim x$, $x \in \dot{x}$, et la réunion de toutes les classes est bien l'ensemble E en entier ; deux plus <u>deux classes distinctes sont disjointes</u>, car si $z \in \dot{x} \cap \dot{y}$, on a $z \sim x$ et $z \sim y$, donc $x \sim z$ et $z \sim y$, donc $x \sim y$, et $x \in \dot{y}$; si $x' \in \dot{x}$ on a de même $x' \sim x$ et $x \sim y$ donc $x' \sim y$ et $x' \in \dot{y}$; autrement dit $\dot{x} \subset \dot{y}$; de même $\dot{y} \subset \dot{x}$, et finalement $\dot{x} = \dot{y}$ dès que $\dot{x} \cap \dot{y} \neq \emptyset$. ■

Les classes de la partition associées à une relation d'équivalence s'appellent <u>classes d'équivalence</u>, et on vient de voir que toute partition est de ce type-là.

L'ensemble des classes d'équivalence s'appelle "<u>ensemble-quotient</u>" ou "<u>quotient</u>" de E par la relation d'équivalence $\sim$, et se note $E/_\sim$. Ses éléments sont les classes de la partition associée ; ce sont donc des <u>sous-ensembles</u> de E.

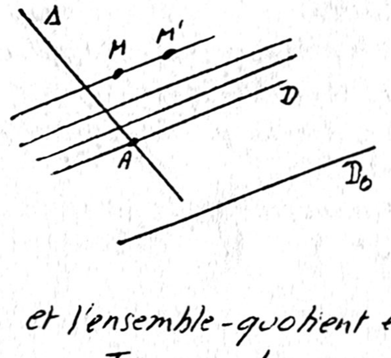
3- Ces définitions abstraites mais naturelles sont en fait fondamentales en mathématiques, et même bien au-delà, et on en fait constamment usage : par exemple les "classes d'âge" d'une population sont les classes de la relation "avoir des âges dans la même tranche" dans l'ensemble des individus ; on emploie couramment une partition des jours en sept classes qui ont nom : lundi, mardi, ..., dimanche ; l'ensemble-quotient de l'équivalence "avoir même nationalité" est l'ensemble des nations ; etc... Il faut d'ailleurs remarquer que dès qu'on considère une application f d'un ensemble X dans un ensemble Y, la relation sur X "avoir même image par f" est une relation d'équivalence, et la donnée de f fournit donc aussitôt une partition de X.

On a déjà utilisé ici plusieurs fois ces notions, et dans des constructions essentielles. Ainsi :

- $\mathbb{Q}$ c'est l'ensemble-quotient $\mathbb{Z}\times\mathbb{Z}^*/\sim$, où $(p,q)\sim(p',q') \Leftrightarrow pq'=p'q$.
- $\mathbb{R}$ est aussi défini comme ensemble-quotient : un nombre réel est une classe d'équivalence de suites de Cauchy de nombres rationnels.
- On verra plus loin (au 6-D-3) que la définition la plus naturelle de $\mathbb{C}$ est aussi un quotient.
- L'ensemble $\mathbb{Z}/n$ des "entiers modulo n" (n donné ≥ 2) a été défini très explicitement comme quotient de $\mathbb{Z}$ par la relation d'équivalence "modulo n" : $p\sim p' \Leftrightarrow n \mid p-p'$.
  On a ensuite muni cet ensemble des opérations "héritées" de celles de $\mathbb{Z}$, pour en faire un anneau. C'est-à-dire que pour effectuer la somme ou le produit de deux classes, on fait ces opérations sur des "représentants" de chaque classe, puis on prend la classe du résultat : $\begin{cases} \bar{\bar{x}} + \bar{\bar{y}} = \overline{\overline{x+y}} \\ \bar{\bar{x}}.\bar{\bar{y}} = \overline{\overline{xy}} \end{cases}$
  (Encore faut-il vérifier que celle-ci ne dépend pas des représentants choisis, pour que les opérations sur le quotient soient bien définies...)

4- Un <u>représentant</u> d'une classe est un élément choisi dans cette classe pour la "représenter", par exemple dans les calculs ci-dessus.
Si l'on choisit un représentant de chaque classe, ils forment un ensemble canoniquement en bijection avec le quotient. Ainsi l'assemblée générale de l'O.N.U. "représente" l'ensemble-quotient des nations (c'est un très mauvais exemple !)

Mais rien n'empêche a priori de changer de représentants (dans les classes démocratiques, du moins) : un représentant, c'est en fait <u>n'importe quel élément</u> d'une classe.



Exemple : dans le plan P donnons-nous une direction de droite D_0 et considérons la relation entre points du plan : $M\sim M'$ si et seulement si le vecteur $\overrightarrow{MM'}$ est parallèle à D_0. On vérifie que c'est une équivalence. Les classes sont toutes les droites D parallèles à D_0 (et dès qu'elles sont distinctes, elles sont disjointes !), et l'ensemble-quotient est donc l'ensemble de ces droites.

Traçons alors une droite Δ qui n'est <u>pas</u> parallèle à D_0 ; elle coupe chaque droite D en un point et un seul A, et $\bar{\bar{A}} = D$; on peut choisir A comme représentant de D et on obtient ainsi une <u>représentation</u> du quotient par la droite Δ. Celle-ci n'a rien de "canonique" : toute autre droite non parallèle à D_0 fait aussi bien l'affaire que Δ.

On peut parfois trouver une représentation <u>canonique</u> d'un ensemble-quotient, et cela vaut alors la peine d'être remarqué. Ainsi :

— un élément r de $\mathbb{Q}$ est représenté par n'importe quelle "fraction" $\frac{p}{q}$, c'est-à-dire n'importe quel couple (p,q) de classe r. Mais une seule

d'entre elles est <u>irréductible</u> ($p\wedge q = 1$ et $q > 0$), et c'est celle-ci qu'on choisira de préférence pour représenter r. (Mais les opérations de $\mathbb{Q}$ ne s'explicitent pas bien dans cette représentation ...)

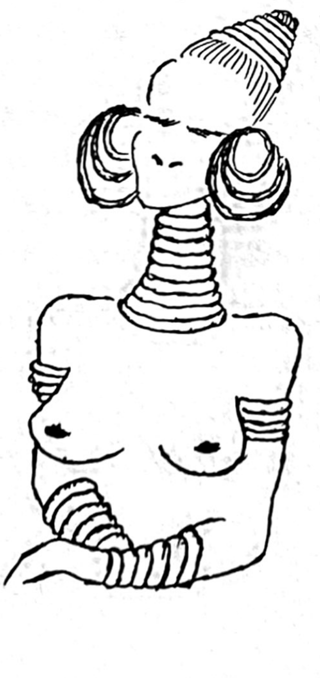
- au paragraphe 1-D on a très vite choisi comme représentant canonique de la classe d'un entier modulo n, le reste de sa division euclidienne par n, c'est-à-dire le seul élément de sa classe dans l'intervalle $[0, n-1]$. Ainsi $\{0, 1, \dots, n-1\}$ est une représentation canonique de $\mathbb{Z}/_n$ (pas si canonique que ça : on aurait pu choisir $[2n, 3n-1]$, ou $[1, n]$, ou $[-n+1, 0]$ ...)
- on représente souvent les "réels modulo 2π", c'est-à-dire les éléments de l'ensemble-quotient $\mathbb{R}/_{2\pi\mathbb{Z}}$, qui servent à "mesurer" les angles orientés (en radians), par les réels de l'intervalle $[0, 2\pi[$; mais il arrive qu'on en choisisse une autre représentation, comme par exemple l'intervalle $]-\pi, \pi]$.

5- Une relation binaire sur un ensemble E qui est réflexive et transitive mais <u>antisymétrique</u> ($\forall x, y \in E$, $x \mathcal{R} y$ et $y \mathcal{R} x \Rightarrow y = x$) s'appelle une <u>relation d'ordre</u> et se note souvent $\leq$. Un ensemble muni d'une relation d'ordre est dit <u>ordonné</u>, et <u>totalement</u> ordonné si deux éléments quelconques sont toujours "comparables" : $\forall x, y \in E$, $x \leq y$ ou $y \leq x$.

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont totalement ordonnés pour la relation $\leq$ habituelle.

<u>Autres exemples</u> : • Sur l'ensemble $\mathcal{P}(E)$ des <u>parties</u> d'un ensemble E, l'inclusion définit une relation d'ordre : $\forall X, Y, Z \in \mathcal{P}(E)$, $X \subset X$; $X \subset Y$ et $Y \subset X \Rightarrow X = Y$; $X \subset Y$ et $Y \subset Z \Rightarrow X \subset Z$.
Cet ordre n'est pas total. Par contre il existe un plus grand élément, et un plus petit : $E = \sup\limits_{X \in \mathcal{P}(E)} X$ et $\emptyset = \inf\limits_{X \in \mathcal{P}(E)} X$.

• Sur l'ensemble $\mathbb{N}$, la relation de division est une relation d'ordre qui admet aussi un plus grand élément, 0, et un plus petit, 1 ; elle n'est pas non plus totale. C'est pour cet ordre-là que le pgcd et le ppcm sont "le plus grand" et "le plus petit".
Sur $\mathbb{Z}$, la relation n'est plus tout-à-fait antisymétrique (c'est ce qu'on appelle une relation de "<u>préordre</u>".)



(Exemple d'anneaux ... et de corps)

DEUXIÈME PARTIE : DES POLYNÔMES

« L'imam et émir des croyants al-Mamun m'a encouragé à composer un ouvrage concis sur le calcul "al-jabr" (= réduction) et "al muqabala" (= comparaison), limité à l'art du calcul agréable et de grand intérêt, dont les gens ont constamment besoin pour leurs héritages, leurs testaments, leurs sentences, leurs transactions... »

(Al Khwarizmi, VIII^e/IX^e siècle)

Les équations algébriques s'écrivent avec des polynômes. On définit proprement cette notion au chapitre 4 (c'est-à-dire qu'on escamote "l'inconnue"). On obtient ainsi un anneau aux propriétés de division remarquables, dont on développe la théorie au chapitre 5.

On peut alors appliquer ces résultats aux problèmes liés aux équations algébriques (à une seule inconnue) : c'est ce qu'on tente au chapitre 6. On n'y obtient que des résultats partiels.

Une extension naturelle de ces méthodes au corps des fractions rationnelles (chapitre 7) donne en particulier un résultat de décomposition indispensable au calcul intégral.

CHAPITRE 4 : L'ANNEAU DES POLYNÔMES

« Nul ne peut dire ce qu'est une variable »
(Hermann Weyl, 1885/1955)

Ⓐ FORMALITÉS

1- Soit K un corps commutatif ; un polynôme de la variable X à coefficients dans K est n'importe quelle combinaison finie des puissances entières naturelles de la lettre X à coefficients dans K, soit :

$$P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_p X^p = \sum_{j=0}^{p} a_j X^j$$

avec $p \in \mathbb{N}$, $a_j \in K$. Si tous les a_j sont nuls, on a le polynôme nul, noté 0. Sinon $\deg P = \sup_{a_j \neq 0} j$ et $\operatorname{val} P = \inf_{a_j \neq 0} j$ sont des entiers naturels bien définis, appelés degré et valuation du polynôme P. Le polynôme nul n'a pas de degré ni de valuation ; on pose souvent par convention $\operatorname{val} 0 = +\infty$ et $\deg 0 = -\infty$, mais quelquefois $\deg 0 = -1$ est plus pratique.

Formellement, un polynôme n'est donc pas autre chose que la donnée de la suite de ses coefficients : $(a_0, a_1, \dots, a_p, 0, 0, \dots)$, et on peut définir un polynôme comme un élément de $K^{\mathbb{N}}$ (c'est-à-dire une application de $\mathbb{N}$ dans K, ou encore une suite à valeurs dans K), dont toutes les valeurs sont nulles sauf un nombre fini. L'ensemble des polynômes se note $K[X]$.

2- L'addition : elle se fait "coefficient par coefficient" : si $P = \sum_{j \in \mathbb{N}} a_j X^j$ et $Q = \sum_{j \in \mathbb{N}} b_j X^j$, par définition $P + Q = \sum_{j \in \mathbb{N}} (a_j + b_j) X^j$.

Autrement dit si P est la suite $(a_j)_{j \in \mathbb{N}}$ et Q la suite (b_j), $P+Q$ est la suite $(a_j + b_j)_{j \in \mathbb{N}}$.

Le polynôme nul est la suite nulle $(0, 0, \dots, 0, \dots)$; si l'on pose $1 = X^0 = (1, 0, 0, \dots, 0, \dots)$, $X = (0, 1, 0, \dots, 0, \dots)$, et plus généralement $X^j = (0, \dots, 0, 1, 0, \dots, 0, \dots)$ (le 1 étant situé à la place numérotée j), tout polynôme est une combinaison (finie) des X^j $(j \in \mathbb{N})$.

L'addition est évidemment associative et commutative, 0 est l'élément neutre, et l'opposé de $P = (a_j)$ est $-P = (-a_j)_{j \in \mathbb{N}}$.

Muni de cette addition $K[X]$ est donc un groupe abélien. De plus, on vérifiera sans peine

$$\boxed{\deg(P+Q) \leq \sup(\deg P, \deg Q)} \quad \text{et} \quad \boxed{\operatorname{val}(P+Q) \geq \inf(\operatorname{val} P, \operatorname{val} Q)}$$

les inégalités étant même des égalités sauf si $\deg P = \deg Q$, ou $\operatorname{val} P = \operatorname{val} Q$.

3- La <u>multiplication</u> est celle que l'on connait bien : si $P=(a_j)$, $Q=(b_j)$, on pose $PQ = (c_j)_{j\in\mathbb{N}}$, avec $c_j = \sum_{i=0}^{j} a_i b_{j-i} = a_0 b_j + a_1 b_{j-1} + \dots + a_j b_0$.

Il vient alors que pour tous $j,k \in \mathbb{N}$, $X^j X^k = X^{j+k}$, ce qui justifie la notation, puis qu'un produit de polynômes se développe "distributivement", c'est-à-dire de la façon habituelle:

$$\Big(\sum_{j\in\mathbb{N}} a_j X^j\Big)\Big(\sum_{k\in\mathbb{N}} b_k X^k\Big) = \sum_{j,k\in\mathbb{N}} a_j b_k X^{j+k} = \sum_{\ell\in\mathbb{N}} \Big(\sum_{i=0}^{\ell} a_i b_{\ell-i}\Big) X^\ell$$

De plus il est clair que

$$\boxed{\begin{aligned} \deg PQ &= \deg P + \deg Q \\ \operatorname{val} PQ &= \operatorname{val} P + \operatorname{val} Q \end{aligned}} \quad (*)$$

La multiplication est associative et distributive par rapport à l'addition; elle est aussi commutative et admet un élément neutre, qui est 1. Muni de ces deux opérations, $K[X]$ est donc un <u>anneau commutatif unitaire</u>, <u>intègre</u> à cause de $(*)$, qui implique aussi que les seuls éléments <u>inversibles</u> de l'anneau sont les polynômes de degré 0, autrement dit les <u>constantes</u> non nulles, $(a_0, 0, \dots, 0, \dots)$ avec $a_0 \neq 0$ (l'inverse est $(a_0^{-1}, 0, \dots, 0, \dots)$.).

L'application $\begin{aligned} K &\longrightarrow K[X] \\ a &\longmapsto (a,0,\dots,0,\dots) \end{aligned}$ est une injection qui permet d'<u>identifier</u> le corps "de base" K à un sous-anneau de $K[X]$: les constantes.

4- L'objet de cette deuxième partie du cours est l'étude des riches propriétés de l'anneau $K[X]$. Mais il n'y a aucune raison de limiter les définitions et remarques précédentes aux polynômes d'<u>une seule</u> variable. Les "systèmes d'équations algébriques" mentionnés dans l'introduction font intervenir des polynômes de <u>plusieurs</u> variables, et tout ce qu'on vient de dire se généralise aussitôt:

Soient $X_1, \dots, X_n$ n lettres distinctes. On notera $K[X_1, \dots, X_n]$ l'ensemble des applications de $\mathbb{N}^n$ dans K dont toutes les valeurs sont nulles sauf un nombre fini, autrement dit l'ensemble des "suites multiples" $(a_{\alpha_1,\dots,\alpha_n})_{(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n}$ dont tous les "termes" $a_{\alpha_1,\dots,\alpha_n}$ appartiennent à K, et sont nuls sauf un nombre fini.

Pour $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, notons $|\alpha| = \alpha_1 + \dots + \alpha_n$, $a_\alpha = a_{\alpha_1,\dots,\alpha_n}$, et $X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ la suite $(a_\beta)_{\beta\in\mathbb{N}^n}$ définie par $\begin{cases} a_\beta = 0 \text{ si } \beta \neq \alpha. \\ a_\alpha = 1 \end{cases}$

Tout "<u>polynôme de n variables</u>" $P \in K[X_1, \dots, X_n]$ s'écrit de façon unique comme combinaison des X^α ($\alpha \in \mathbb{N}^n$; $X^0 = 1$), pour une somme et un

produit définis par les formules

$$\begin{cases} \left(\sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha\right) + \left(\sum_{\alpha\in\mathbb{N}^n} b_\alpha X^\alpha\right) = \sum_{\alpha\in\mathbb{N}^n} (a_\alpha + b_\alpha) X^\alpha \\ \left(\sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha\right)\left(\sum_{\beta\in\mathbb{N}^n} b_\beta X^\beta\right) = \sum_{\gamma\in\mathbb{N}^n} c_\gamma X^\gamma, \text{ avec } c_\gamma = \sum_{\substack{\alpha,\beta\in\mathbb{N}^n;\\ \alpha+\beta=\gamma}} a_\alpha b_{\beta-\alpha} \end{cases}$$

qui munissent $K[X_1,\ldots,X_n]$ d'une structure d'anneau commutatif unitaire. De plus si l'on pose $\deg(\sum a_\alpha X^\alpha) = \sup_{a_\alpha\neq 0} |\alpha|$ et $\operatorname{val}(\sum a_\alpha X^\alpha) = \inf_{a_\alpha \neq 0} |\alpha|$, on obtient les mêmes formules qu'aux numéros 2 et 3, et (*) démontre encore que $K[X_1,\ldots,X_n]$ est <u>intègre</u> et que ses éléments <u>inversibles</u> sont les constantes non nulles (polynômes de degré 0).

Toutefois ce sont les polynômes d'une seule variable, c'est-à-dire l'anneau $K[X]$, qu'on étudie ici ; ceux de plusieurs variables ne seront cités que pour fournir quelques exemples.

⌈Enfin remarquons que pour définir l'anneau $K[X]$ comme on l'a fait ici, il n'est pas nécessaire que K soit un corps : on peut prendre un <u>anneau</u> A, et vérifier que $A[X]$ est commutatif, unitaire, et intègre dès que A l'est. L'anneau $\mathbb{Z}[X_1,\ldots,X_n]$ est d'ailleurs celui qui intervient dans les équations diophantiennes.⌋

(B) POLYNÔME ET FONCTION POLYNÔME

1 - A tout polynôme $P\in K[X]$ est naturellement associée une <u>fonction polynôme</u> $\tilde{P}$, application de K dans K : sa valeur au point $x\in K$ est $\tilde{P}(x) = \sum_{j=1}^{p} a_j x^j$ si $P(X) = \sum_{j=1}^{p} a_j X^j$. Comme dans K $x^i x^j = x^{i+j}$ pour $i,j\in\mathbb{N}$, l'application $K[X] \to K^K$, $P \mapsto \tilde{P}$ respecte somme et produit : $\widetilde{P+Q} = \tilde{P}+\tilde{Q}$; $\widetilde{PQ} = \tilde{P}\tilde{Q}$.

6] Ce sont les fonctions polynômes qu'on a déjà étudiées depuis longtemps (du moins lorsque $K=\mathbb{R}$), mais qu'il y ait lieu de distinguer résulte de ce que l'application ci-dessus n'est pas toujours injective : par exemple si $K=\mathbb{Z}/3$, le polynôme $P = X^3+2X = X(X-1)(X-2)$ n'est <u>pas</u> le polynôme nul, puisque c'est la suite $(0,2,0,1,0,\ldots,0,\ldots)$ et que $\operatorname{val} P = 1$, $\deg P = 3$; alors que la fonction $\tilde{P}$ est la fonction nulle.

Toutefois l'application $P\mapsto\tilde{P}$ est injective pour $K=\mathbb{Q},\mathbb{R},\mathbb{C}$, et plus généralement dès que K est infini, comme on le verra en 6-A-3. Dans ce cas $K[X]$ s'identifie à un sous-anneau de K^K formé des fonctions "polynômes", et on se permet d'écrire P au lieu de $\tilde{P}$.

Rappelons que notre motivation est la recherche des <u>solutions</u> d'une équation algébrique, c'est-à-dire des <u>zéros</u> d'une fonction polynôme, qu'on appellera <u>racines</u> du polynôme.

2- Lorsque $K=\mathbb{R}$, il est bien connu que les fonctions polynômes sont dérivables, la dérivée en un point étant définie comme la limite que l'on sait, et la fonction dérivée étant encore une fonction polynôme.

Mais il y a lieu de remarquer ici que la dérivation peut se définir formellement comme une application $P \mapsto P'$ de $K[X]$ dans $K[X]$, et ceci quel que soit le corps K : c'est la seule application qui vérifie les trois propriétés suivantes : $\forall a \in K, \forall P, Q \in K[X]$

$$\begin{cases} (1)\ (P+Q)' = P'+Q' \\ (2)\ (aX)' = a \\ (3)\ (PQ)' = P'Q+PQ' \end{cases}$$

Preuve : D'abord $a=(aX)'=a'X+aX'=a'X+a$, d'où $a'X=0$ puis $a'=0$ (intégrité) : la dérivée d'une constante est nulle, et (3) implique alors $(aP)'=aP'$, puis par (1) et (3) $(aP+bQ)'=aP'+bQ'$, et finalement $(\sum a_j X^j)' = \sum a_j (X^j)'$.

Que $(X^j)' = jX^{j-1}$ (pour $j \in \mathbb{N}$, le j du second membre signifiant $j.1 \in K$), se prouve par récurrence sur j à l'aide de (2) et (3) :

$$(X^j)' = (X.X^{j-1})' = X'.X^{j-1} + X(X^{j-1})' = 1.X^{j-1} + (j-1)X.X^{j-2} = jX^{j-1}.$$

On a ainsi retrouvé que : $\boxed{\left(\sum_{j=0}^{p} a_j X^j\right)' = \sum_{j=0}^{p} j a_j X^{j-1}}$ ■

P dérivé n fois se notant $P^{(n)}$ dès que $n \geq 3$, notons que $\deg P' = \deg P - 1$ pour P non constant, puis $\deg P^{(n)} = \deg P - n$ dès que $\deg P \geqslant n$; si $\deg P = p$, $P^{(p)}$ est la constante $p!\,a_p$.

L'utile formule de Leibniz :

$$\forall P, Q \in K[X], \forall n \in \mathbb{N} \qquad \boxed{(PQ)^{(n)} = \sum_{j=0}^{n} C_n^j P^{(j)} Q^{(n-j)}} \qquad C_n^p = \frac{n!}{p!(n-p)!}$$

se démontre facilement par récurrence sur l'entier n.

Elle permet par exemple d'écrire, sans calcul superflu, que :

$$(X^3.P)^{(4)} = X^3.P^{(4)} + 12X^2.P''' + 36X.P'' + 24P'.$$

3- Dans ce numéro, on suppose K de caractéristique nulle : les entiers écrits sont donc de "vrais" entiers ; en particulier pour tout $j \in \mathbb{N}$, $j! \in K$ est non nul, donc inversible (on pose comme d'habitude $0!=1$)

On dispose alors de l'identité de Taylor :

$$\forall a \in K, \forall P \in K[X] \qquad \boxed{P(X) = \sum_{j \in \mathbb{N}} \frac{P^{(j)}(a)}{j!}(X-a)^j}$$

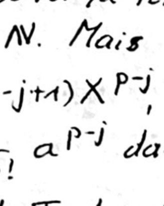
(Notons que comme $\#K = \infty$, on a noté $P^{(j)}(a)$ au lieu de $\tilde{P}^{(j)}(a)$.)

Preuve : Les propriétés de la dérivation vues au 2, et le fait que $(\tilde{P})' = \widetilde{(P')}$ montrent qu'il suffit de prouver la formule pour un "monôme", puis dans le cas où $P = X^p$ avec $p \in \mathbb{N}$. Mais $X^p = (X-a+a)^p = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} a^{p-j}(X-a)^j$.

Comme $(X^p)^{(j)} = p(p-1)\cdots(p-j+1)X^{p-j}$,

on a bien $P^{(j)}(a) = \frac{p!}{(p-j)!} a^{p-j}$ dans ce cas. ■

Dans l'identité de Taylor, la somme $\sum_{j \in \mathbb{N}}$ est en fait une somme finie, puisque toutes les dérivées de P d'ordre plus grand que son degré sont nulles.



CHAPÎTRE 5 : THÉORIE DE LA DIVISION

« Pour partir nombre rompu, premier faut reduire, et savoir ce que vault ce que vous voulez partir, et ce par qui le voulles partir, et apres partir comme se ils fussent entiers »

(Nicolas Chuquet, le "Kadran aux marchans", 1485)

(A) EUCLIDE, BEZOUT, ET GAUSS

1- Théorème de division euclidienne :

$\forall A, B \in K[X], B \neq 0, \exists 1 (Q, R), A = BQ + R$ et $\deg R < \deg B$ ou $R = 0$

Preuve : L'existence se montre par récurrence sur $\deg A = p$. Posons $q = \deg B$. Dès que $p < q$, ou si $A = 0$, on peut prendre $Q = 0$ et $R = A$. Sinon $p = q + r$, avec $r \in \mathbb{N}$. Si alors les termes de plus haut degré de A et B sont respectivement $a_p X^p$ et $b_q X^q$, on a $A = \left(\frac{a_p}{b_q} X^r\right) . B + A_1$ avec $\deg A_1 < p$, donc $A_1 = BQ_1 + R_1$ et $\deg R_1 < q$ ou $R_1 = 0$, par hypothèse de récurrence. Il vient alors $A = BQ + R_1$, avec $Q = \frac{a_p}{b_q} X^r + Q_1$.

Si maintenant $BQ + R = BQ' + R'$ avec $\deg R < q$, $\deg R' < q$ (s'ils ne sont pas nuls), on a $B(Q - Q') = R' - R$. Dès que $Q - Q' \neq 0$, le terme de gauche est de degré $\geq q$. Donc $Q = Q'$, et $R = R'$. ■

2- Q et R s'appellent le quotient et le reste de la division euclidienne de A par B, et la preuve du 1 fournit en fait un algorithme pour les calculer : on ordonne les polynômes "puissances décroissantes" et on pose la division

$$
\begin{array}{l|l}
a_p X^p + a_{p-1} X^{p-1} + \cdots + a_0 & b_q X^q + b_{q-1} X^{q-1} + \cdots + b_0 \\
\hline
-\left(\frac{a_p}{b_q} X^r\right)(b_q X^q + \cdots + b_0) & \frac{a_p}{b_q} X^r + \cdots \\
\hline
= \quad A_1 \text{ de degré } \leq p-1 & \\
\quad \vdots &
\end{array}
$$

Tant que le degré de ce qui reste en bas à gauche est $\geq q$, on peut continuer. Dès qu'il est $< q$, on a obtenu le reste ... donc aussi le quotient en bas à droite. Exemple : (en supposant carac $K \neq 2$)

$$
\begin{array}{r|l}
X^5 - 2X^4 \quad + 3X^2 - 5X + 1 & 2X^2 - 4X + 1 \\
\hline
-(X^5 - 2X^4 + \frac{1}{2}X^3) & \frac{1}{2}X^3 - \frac{1}{4}X + 1 \\
\hline
-\frac{1}{2}X^3 + 3X^2 - 5X + 1 & \\
-(-\frac{1}{2}X^3 + X^2 - \frac{1}{4}X) & \\
\hline
2X^2 - \frac{19}{4}X + 1 & \\
-(2X^2 - 4X + 1) & \\
\hline
-\frac{3}{4}X &
\end{array}
$$

Soit : $\underbrace{X^5 - 2X^4 + 3X^2 - 5X + 1}_{A} = \underbrace{(2X^2 - 4X + 1)}_{B} \underbrace{(\tfrac{1}{2}X^3 - \tfrac{1}{4}X + 1)}_{Q} \underbrace{- \tfrac{3}{4}X}_{R}$

3- Remarques: (1) ⌜On voit qu'au cours de la division, on n'a jamais à inverser que le scalaire b_q. Si $b_q = 1$ (on dit alors que B est unitaire), le calcul vaut donc aussi lorsque K est seulement un anneau.⌟

(2) Le théorème, et l'algorithme de calcul, sont les mêmes quel que soit le corps K. Mais l'allure du calcul peut en dépendre. Par exemple si $K = \mathbb{Z}/2$, l'exemple précédent devient
$$\begin{array}{l|l} X^5+X^2+X+1 & 1 \\ \hline 0 & X^5+X^2+X+1 \end{array} \quad !$$

(3) On dit que B divise A, ou que A est un multiple de B lorsque le reste de la division euclidienne de A par B est nul; on écrira ici $B \mid A$, et cette relation de division est une relation de préordre (réflexive et transitive).
Tout le monde divise 0, et 0 ne divise que 0. 1, ou plus généralement un inversible (= une constante non nulle) divise tout le monde.

(4) Si $B \mid A$ et $A \mid B$ (supposons l'un non nul; alors l'autre aussi), c'est que $A = BQ$ et $B = AP$ pour certains $P, Q \in K[X]$. Donc $A(QP-1) = 0$, et $PQ = 1$; les quotients sont donc des constantes inverses l'une de l'autre.
Si l'on se restreint au sous-ensemble des polynômes unitaires, la relation de division devient une vraie relation d'ordre.

4- Corollaire: Soit $a \in K$ et $P \in K[X]$. Alors a est racine de P (c'est-à-dire $P(a) = 0$) si et seulement si $X-a$ divise $P(X)$.

Preuve: La division euclidienne de P par $X-a$ s'écrit $P(X) = (X-a)Q(X) + R$, avec $R = 0$ ou $\deg R < 1$; donc R est une constante r, nulle ou non. Au point a, la fonction associée vaut donc $P(a) = r$, et $X-a \mid P \Leftrightarrow r = 0 \Leftrightarrow P(a) = 0$. ∎

5- Une partie non vide $I \subset K[X]$ est appelée un idéal si elle est "stable par différences et par multiples": $\begin{cases} \forall A, B \in I,\ A - B \in I \\ \forall A \in I, \forall P \in K[X],\ PA \in I \end{cases}$

Soit $A \in I$. Alors $0 = A - A \in I$, $-A = 0 - A \in I$, et si $B \in I$, $A+B = B-(-A) \in I$. Donc I est en particulier un sous-groupe de $K[X]$ pour l'addition.

5] L'intersection de deux (ou plusieurs) idéaux est encore un idéal, de même que leur somme $I + J = \{P+Q \mid P \in I, Q \in J\}$, mais pas leur réunion.

L'ensemble des multiples d'un polynôme donné A est un idéal, noté I_A ou $\langle A \rangle$, et appelé l'idéal engendré par A. Plus généralement, l'ensemble des combinaisons de n polynômes donnés $A_1, \dots, A_n$ à coefficients polynômes, soit $\{P_1A_1 + \dots + P_nA_n \mid P_1, \dots, P_n \in K[X]\}$ $= I_{A_1,\dots,A_n} = I_{A_1} + I_{A_2} + \dots + I_{A_n} = \langle A_1, \dots, A_n \rangle$ est donc un idéal, appelé l'idéal engendré par $A_1, \dots, A_n$. On dit que $\{A_1, \dots, A_n\}$ en est un système de générateurs.

Un idéal engendré par un seul générateur est dit monogène. Dans ce cas, son générateur est unique à un facteur constant non nul près, d'après la remarque (4) du 3.

6- Théorème: Tout idéal de $K[X]$ est monogène.

Preuve: Soit I un idéal de $K[X]$. $I \ni 0$. Si $I=\{0\}$, $I=\langle 0\rangle$. Sinon $I^*=I-\{0\}$ est non vide, et l'ensemble $\{\deg P \mid P\in I^*\}$ est une partie non vide de $\mathbb{N}$, qui a un plus petit élément $p\geq 0$, qui est le degré d'un certain $B\in I^*$.
Soit maintenant $A\in I$; par le théorème de division euclidienne, on peut écrire $A=BQ+R$ avec $R=0$ ou $\deg R<p$. Mais $A\in I$, $B\in I$, donc $R=A-BQ\in I$, et $\deg R\geq p$ ou $R=0$. Donc $R=0$, et $A=BQ\in\langle B\rangle$.
Finalement $I=\langle B\rangle$. ■

7- Soient $A_1,\dots,A_n$ des polynômes, et B un diviseur commun: $B|A_1,\dots,B|A_n$. Alors B divise toute combinaison $A_1U_1+\dots+A_nU_n$, avec $U_1,\dots,U_n\in K[X]$, et réciproquement. Par le théorème 6, il existe Δ, d'ailleurs unique à un facteur constant près, tel que $\langle A_1,\dots,A_n\rangle=\langle\Delta\rangle$, autrement dit tel que toute combinaison de $A_1,\dots,A_n$ soit un multiple de Δ et réciproquement. En particulier Δ est un diviseur commun de $A_1,\dots,A_n$, et tout diviseur commun divise Δ. On appelle Δ le plus grand commun diviseur (p.g.c.d.) de $A_1,\dots,A_n$, et on le notera ici $A_1\wedge\dots\wedge A_n$.

Par exemple le pgcd de X^2-1 et X^2+2X+1 est $X+1$ (du moins si carac $K\neq 2$; sinon c'est $X^2-1=X^2+1=X^2+2X+1$!)

Le pgcd n'est défini qu'à un facteur constant (non nul) près, et on pourrait, pour le définir complètement, poser qu'un pgcd est toujours un polynôme unitaire.
Il est clair que $A\wedge 0=A$ et $A\wedge 1=1$; il est clair aussi que $A\wedge B=B\wedge A$ et que $A_1\wedge A_2\wedge\dots\wedge A_n=(\dots((A_1\wedge A_2)\wedge A_3)\dots)\wedge A_n$.

8- Si $\Delta=A_1\wedge\dots\wedge A_n$, en particulier $\Delta\in\langle A_1,\dots,A_n\rangle$, autrement dit:

(*) $\forall A_1,\dots,A_n\in K[X]$, $\exists U_1,\dots,U_n\in K[X]$, $A_1U_1+\dots+A_nU_n=A_1\wedge\dots\wedge A_n$
("identité de Bezout")

On dit que $A_1,\dots,A_n$ sont premiers entre eux s'ils n'ont pas de diviseur commun non trivial, autrement dit si $A_1\wedge\dots\wedge A_n=1$

Proposition: (identité de Bezout) Pour $A_1,\dots,A_n\in K[X]$,
$$A_1\wedge\dots\wedge A_n=1 \Leftrightarrow \exists U_1,\dots,U_n\in K[X],\ A_1U_1+\dots+A_nU_n=1$$

Preuve: $\Rightarrow$ est clair ; $\Leftarrow$ aussi car si $I=\langle A_1,\dots,A_n\rangle\ni 1$, I contient tout multiple de 1, donc $I=K[X]=\langle 1\rangle$. ■

En particulier pour deux polynômes A et B, il est équivalent de dire qu'ils n'ont aucun diviseur commun autre que les constantes, ou qu'il existe U et V tels que $AU+BV=1$.

⟦ Par exemple, si carac $K\neq 3$, X^2+2X et X^2-1 sont premiers entre eux, puisque $1=(X^2+2X)(\frac{2}{3}X-\frac{1}{3})-(X^2-1)(\frac{2}{3}X+1)$. Par contre si carac $K=3$, ils ont le diviseur commun évident $X+2=X-1$, qui est d'ailleurs leur pgcd. ⟧

Résoudre une "équation de Bezout", c'est trouver, pour $A_1,\dots,A_n$ donnés, toutes les familles de polynômes $U_1,\dots,U_n$ solutions de (*). Le

numéro suivant fournit un algorithme de calcul d'un pgcd et d'une solution particulière d'une équation de Bezout. L'associativité implique qu'il suffit de savoir traiter le cas de deux polynômes A et B.

9- <u>L'algorithme d'Euclide</u>

Si $A=BQ+R$, les diviseurs communs de A et B sont les mêmes que ceux de B et R, donc $A\wedge B = B\wedge R$. Effectuons les divisions euclidiennes successives (supposons $B\neq 0$) : $B=R_0$; $A=BQ_1+R_1$, $B=R_1Q_2+R_2, \dots, R_{n-2}=R_{n-1}Q_n+R_n$, avec $\deg B > \deg R_1 > \deg R_2 > \dots > \deg R_n$. Tant que le reste trouvé est non nul, on peut continuer, et comme la suite $(\deg R_j)$ est une suite d'entiers strictement décroissante, "ça s'arrête" : $\exists n$, $R_{n+1}=0$, donc $R_{n-1}=Q_{n+1}R_n$. Il vient alors $A\wedge B = B\wedge R_1 = \dots = R_{n-1}\wedge R_n = R_n$, et <u>le pgcd de A et B est donc le dernier reste non nul de cette suite de divisions euclidiennes</u>.

Exemple : soit à calculer $(X^5-1)\wedge(X^3-1)$

$$X^5-1 \,\big|\, X^3-1 \text{ : quotient } X^2,\ \text{reste } X^2-1 \; ; \quad X^3-1 \,\big|\, X^2-1 \text{ : quotient } X,\ \text{reste } X-1 \; ; \quad X^2-1 \,\big|\, X-1 \text{ : quotient } X+1,\ \text{reste } 0$$

$$\Rightarrow (X^5-1)\wedge(X^3-1) = X-1$$

Mais l'algorithme fournit aussi "en remontant le calcul" une solution particulière (U,V) de l'équation de Bezout $AU+BV=A\wedge B$. Ici par exemple :

$$X-1 = (X^3-1) - X(X^2-1) = (X^3-1) - X[(X^5-1) - X^2(X^3-1)]$$
$$= (X^3-1)(X^3+1) - (X^5-1)X, \text{ d'où } U=-X \text{ et } V = X^3+1.$$

[Exercice : démontrer que $(X^p-1)\wedge(X^q-1) = X^{p\wedge q}-1$, pour tous $p,q\in\mathbb{N}$.]

10- On énonce ici le "<u>théorème de Gauss</u>" sous deux formes équivalentes :

<u>Première forme</u> : $\forall A,B,C \in K[X]$, $A|BC$ et $A\wedge B=1 \Rightarrow A|C$

Preuve : $\exists U,V,W\in K[X]$, $AU+BV=1$ et $BC=AW$. D'où $C=ACU+BCV=A(CU+VW)$. ■

<u>Deuxième forme</u> : $\forall A,B,C \in K[X]$, $A\wedge B=1$, $A|C$ et $B|C \Rightarrow AB|C$

Preuve : $\exists U\in K[X]$, $C=AU$, donc $B|AU$ et $A\wedge B=1$, donc $B|U$: $\exists V$, $U=BV$, et $C=ABV$ ■

Une application importante du théorème de Gauss est la résolution complète d'une équation de Bezout. On n'explicite ici que le cas le plus aisé, de deux polynômes A et B premiers entre eux. L'algorithme d'Euclide du 9 fournit une première solution (U_0,V_0) de l'équation $AU+BV=1$. Si (U,V) en est une autre, on a $AU_0+BV_0=1=AU+BV$, d'où $A(U-U_0)=B(V_0-V)$, et $B|A(U-U_0)$. Comme $A\wedge B=1$, $B|U-U_0$, soit $U-U_0=BW$ avec $W\in K[X]$, d'où $ABW=B(V_0-V)$, et si $B\neq 0$ $V_0-V=AW$. Finalement $\{(U=U_0+WB, V=V_0-WA)\}$ où $W\in K[X]$ est l'ensemble des solutions, puisque réciproquement $AU+BV = AU_0+AWB+BV_0-BWA = AU_0+BV_0=1$. ■

11- Si $A_1,\dots,A_n$ sont des polynômes, l'intersection $I_{A_1}\cap\dots\cap I_{A_n}$ est encore un idéal, donc de la forme I_M, avec $M\in K[X]$. C'est dire

que l'ensemble des multiples communs de $A_1, \dots, A_n$ n'est autre que l'ensemble des multiples de M. M est donc le <u>plus petit commun multiple</u> (p.p.c.m) de $A_1, \dots, A_n$, noté ici $A_1 \vee \dots \vee A_n$. Lui aussi n'est défini qu'à un facteur près.

Pour tout $A \in K[X]$, on a $A \vee 0 = 0$ et $A \vee 1 = A$. Il est clair aussi que $A \vee B = B \vee A$ et que $A_1 \vee A_2 \vee \dots \vee A_n = (\dots(A_1 \vee A_2) \vee \dots) \vee A_n$. Un algorithme de calcul des ppcm peut donc se déduire de l'algorithme d'Euclide de calcul des pgcd, et de la formule : <u>$\forall A, B$ non nuls</u>

$$\boxed{A \vee B = \frac{AB}{A \wedge B}}$$

qui se prouve ainsi : si $A \wedge B = 1$, $A \vee B = AB$ (Gauss) ;
si $A \wedge B = \Delta$, $A = \Delta A'$ et $B = \Delta B'$ avec $A' \wedge B' = 1$, d'où :

$$A \vee B = \Delta A' \vee \Delta B' = \Delta (A' \vee B') = \frac{\Delta A' \cdot \Delta B'}{\Delta} = \frac{AB}{A \wedge B}. \blacksquare$$

12- L'analogue du "<u>problème chinois</u>" posé (et résolu) en 1-D-4 est le suivant : étant donnés des polynômes $P_1, \dots, P_n$ et $A_1, \dots, A_n$, trouver tous les polynômes P tels que $P - A_j$ soit divisible par P_j, pour $j = 1, \dots, n$. On se contente ici de traiter le cas $n = 2$ et $P_1 \wedge P_2 = 1$.

Si $P = A_1 + P_1 Q_1 = A_2 + P_2 Q_2$, c'est que $A_1 - A_2 = P_2 Q_2 - P_1 Q_1$ (*)
Comme $P_1 \wedge P_2 = 1$, on peut calculer par l'algorithme d'Euclide des polynômes $\overline{Q_1}, \overline{Q_2}$ tels que $P_2 \overline{Q_2} - P_1 \overline{Q_1} = 1$ (**).
De (*) et (**) on déduit $P_2 [Q_2 - (A_1 - A_2)\overline{Q_2}] = P_1 [Q_1 - (A_1 - A_2)\overline{Q_1}]$
Comme $P_1 \wedge P_2 = 1$, P_2 divise $Q_1 - (A_1 - A_2)\overline{Q_1} = P_2 R$, et en reportant $Q_2 - (A_1 - A_2)\overline{Q_2} = P_1 R$; réciproquement pour tout polynôme R, le couple $(Q_1 = (A_1 - A_2)\overline{Q_1} + P_2 R,\ Q_2 = (A_1 - A_2)\overline{Q_2} + P_1 R)$ est solution de (*), et il suffit donc de poser $P = A_1 + P_1 (A_1 - A_2)\overline{Q_1} + R P_1 P_2 = A_2 + P_2 (A_1 - A_2)\overline{Q_2} + R P_1 P_2$ pour avoir toutes les solutions du problème chinois dans ce cas. $\blacksquare$

⟦ Exemple : trouver tous les polynômes $P \in K[X]$ tels que $X^2 - 1 \mid P - 1$ et $X^3 \mid P + 1$.
(Réponse : $P(X) = 2X^4 - 1 + X^3 (X^2 - 1) R(X)$, où $R \in K[X]$ est arbitraire.) ⟧

(B) <u>FACTORISATION IRRÉDUCTIBLE</u>

1- On appelle <u>irréductible</u> un polynôme non constant qui n'a aucun diviseur non trivial : P irréductible et $P = P_1 P_2 \Rightarrow \deg P_1 = 0$ ou $\deg P_2 = 0$.
Si P est irréductible, pour tout polynôme Q, on a $P \wedge Q = 1$ ou P
Par exemple <u>tout polynôme de degré 1 est irréductible</u>.

2- <u>Théorème</u> : <u>Tout polynôme non nul $P \in K[X]$ s'écrit de façon unique à l'ordre près des facteurs</u> $P = a P_1 P_2 \cdots P_q$, <u>où $a \in K^*$</u>, et les P_j <u>($j = 1, \dots, q$) sont des polynômes irréductibles unitaires</u>.

Preuve : a est le coefficient du terme de plus haut degré de P. On peut supposer P unitaire et $a=1$. Si $P_1 \dots P_q = Q_1 \dots Q_{q'}$, où les P_i et les Q_j sont irréductibles et unitaires, $P_1 \mid Q_1 \dots Q_{q'}$. Comme $P_1 \wedge Q_1 = 1$ ou $P_1 = 1$ ou Q_1, ou bien $P_1 = Q_1$, ou bien $P_1 \mid Q_2 \dots Q_{q'}$ (Gauss), et on peut recommencer jusqu'à conclure que P_1 est l'un des Q_j... On achève la preuve de l'unicité de la décomposition en rédigeant une double récurrence. L'existence se montre aussi par récurrence sur le degré de P. ■

3- On peut bien sûr regrouper les facteurs égaux de la décomposition, et écrire $P = a P_1^{\alpha_1} \dots P_m^{\alpha_m}$, où $a \in K^*$, les α_j sont des entiers, et les P_j sont irréductibles, unitaires et <u>distincts</u>. On appelle α_j la <u>multiplicité</u> du facteur P_j dans P. On peut formaliser cela de la façon suivante : soit $\mathcal{P}$ l'ensemble de tous les polynômes irréductibles unitaires.
Pour tout $P \in K[X]$, il existe une et une seule application $\alpha : \mathcal{P} \to \mathbb{N}$, qui ne prend qu'un nombre fini de fois une valeur non nulle, telle qu'il existe $a \in K^*$ tel que $P = a \prod_{R \in \mathcal{P}} R^{\alpha(R)}$

Avec ces notations, si $P = \prod R^{\alpha(R)}$ et $Q = \prod R^{\beta(R)}$, on a évidemment $P \wedge Q = \prod R^{\inf(\alpha(R), \beta(R))}$ et $P \vee Q = \prod R^{\sup(\alpha(R), \beta(R))}$.

Mais connait-on bien l'ensemble $\mathcal{P}$? Et dispose-t-on d'un algorithme de <u>calcul</u> des facteurs irréductibles d'un polynôme donné ? Les réponses à ces questions, souvent négatives, dépendent du corps de base K.

4- <u>Proposition : Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.</u>
Preuve : Soit $P \in \mathbb{C}[X]$ non constant. Par le théorème de d'Alembert, il a au moins une racine $a \in \mathbb{C}$, et par le corollaire A-4, $P = (X-a)Q$, où $\deg Q = \deg P - 1 > 0$ dès que $\deg P > 1$. ■

<u>Remarque</u> : Le théorème 2 s'énonce donc dans ce cas :
Tout polynôme $P \in \mathbb{C}[X]$ de degré $p > 0$ s'écrit de manière unique $P = a(X-a_1)^{m_1} \dots (X-a_q)^{m_q}$, avec $a \in K^*$; $a_1, \dots, a_q \in K$ distincts ; $m_1 + \dots + m_q = p$. On appelle m_j la <u>multiplicité</u> (ou <u>ordre</u>) de la racine a_j, et on dit que a_j est racine <u>simple</u> de P si $m_j = 1$, <u>double</u> si $m_j = 2$, ..., <u>multiple</u> dès que $m_j > 1$.

5- Remarquons que si $P = \sum_{j=0}^{p} a_j X^j \in \mathbb{R}[X] \subset \mathbb{C}[X]$, avec une racine complexe $a \in \mathbb{C}$ il a <u>aussi</u> la racine conjuguée $\bar{a}$ puisque
$P(\bar{a}) = \sum_{j=0}^{p} a_j \bar{a}^j = \overline{\sum a_j a^j} = \overline{P(a)} = \bar{0} = 0$.

Comme $(X-b) \wedge (X-\bar{b}) = 1$ dès que $b \neq \bar{b}$, donc dès que $b \notin \mathbb{R}$, chaque fois que $P \in \mathbb{R}[X]$ a une racine complexe <u>non réelle</u> b, il est divisible par $X-b$ et par $X-\bar{b}$, donc par $(X-b)(X-\bar{b}) = X^2 - (2\,\mathrm{Re}\, b)X + |b|^2 = P_b(X) \in \mathbb{R}[X]$. Donc $P = P_b \cdot Q$ avec $Q \in \mathbb{R}[X]$, et en itérant,

on voit que les racines b et $\bar{b}$ ont <u>même multiplicité</u>, et que tout $P \in \mathbb{R}[X]$ s'écrit de façon unique $P = c(X-a_1)^{m_1} \cdots (X-a_q)^{m_q} \cdot P_{b_1}^{n_1} \cdots P_{b_r}^{n_r}$,

où $c \in \mathbb{R}^*$; $a_1, \dots, a_q \in \mathbb{R}$ distincts sont les racines réelles de P, de multiplicités $m_1, \dots, m_q$; $b_1, \bar{b}_1, \dots, b_r, \bar{b}_r$ sont les racines complexes <u>non</u> réelles de P, de multiplicités $n_1, \dots, n_r$; et $m_1 + \dots + m_q + 2n_1 + \dots + 2n_r = \deg P$ (supposé $\neq 0$)

En particulier, on a décomposé tout polynôme de $\mathbb{R}[X]$ en produit de polynômes de $\mathbb{R}[X]$ de degrés 1 et 2.

<u>Proposition</u>: <u>Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et ceux de degré 2 de discriminant strictement négatif.</u>

Preuve : il reste seulement à vérifier que ces derniers sont irréductibles. Mais dès qu'un polynôme de degré 2 ne l'est pas, il est le produit de deux polynômes de degré 1 à coefficients <u>réels</u>, donc a deux racines réelles, distinctes ou non. ■

6 - Sur d'autres corps, il peut y avoir des irréductibles de <u>tout</u> degré. Donnons ici deux exemples de décomposition sur $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$:

- $P_1 = X^4 + X^3 + 2X^2 + X + 1 \in \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.
  Sur $\mathbb{R}$ sa décomposition est $P_1 = (X^2+1)(X^2+X+1)$, et c'est aussi sa décomposition sur $\mathbb{Q}$, puisque les deux facteurs sont dans $\mathbb{Q}[X]$, et irréductibles sur $\mathbb{Q}$ puisqu'ils le sont déjà sur $\mathbb{R}$. Mais sur $\mathbb{C}$, $P_1 = (X-i)(X+i)(X-j)(X-j^2)$.
- $P_2 = X^4 + 1 = (X - e^{i\frac{\pi}{4}})(X - e^{\frac{3i\pi}{4}})(X - e^{\frac{5i\pi}{4}})(X - e^{\frac{7i\pi}{4}})$ sur $\mathbb{C}$
  donc $= (X^2 - 2\cos\frac{\pi}{4} X + 1)(X^2 - 2\cos\frac{3\pi}{4} X + 1) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ sur $\mathbb{R}$,
  les deux trinômes étant de discriminant -2.
  Mais P_2 est irréductible sur $\mathbb{Q}$, car
  - s'il avait un facteur de degré 1, il aurait une racine rationnelle (or on connaît toutes ses racines complexes et aucune n'est réelle)
  - si c'était le produit de deux polynômes de degré 2 dans $\mathbb{Q}[X] \subset \mathbb{R}[X]$, ce seraient donc les deux trinômes ci-dessus, par unicité de la décomposition sur $\mathbb{R}$; or ceux-ci ne sont pas à coefficients rationnels.

Ⓒ <u>UNE AUTRE DIVISION</u>

Ⓒ 1 - On peut préciser l'identité de Bezout de la façon suivante :

<u>Théorème</u>: <u>Soient $A, B, C \in K[X]$ tels que $B \wedge C = 1$</u>
<u>$\exists ! \, (Q, R)$, $A = BQ + CR$ et $\deg Q < \deg C$, ou $Q = 0$</u>

Preuve : D'après A-8, il existe Q_0 et $R_0 \in K[X]$ tels que $BQ_0 + CR_0 = 1$, et posant $Q_1 = AQ_0$, $R_1 = AR_0$, on a une première solution de $A = BQ + CR$ (*).
Si (Q_2, R_2) en est une autre, il vient $B(Q_1 - Q_2) = C(R_2 - R_1)$, et $C \mid B(Q_1 - Q_2)$, donc par le théorème de Gauss, $Q_1 - Q_2 = CS$, pour un certain $S \in K[X]$, et par suite $R_2 - R_1 = BS$. Les solutions de (*) sont donc les couples de la forme $(Q = Q_1 - CS, R = R_1 + BS)$, où S est arbitraire. Si de plus $\deg Q < \deg C$ ou $Q = 0$, comme $Q_1 = Q + CS$, c'est que S et Q sont le quotient et le reste de la division euclidienne de Q_1 par C ; d'où le résultat. ■

La preuve donne en même temps un algorithme de calcul du couple (Q, R) solution : on a vu en A-9 comment l'algorithme d'Euclide permet de calculer (Q_0, R_0), donc (Q_1, R_1) ; S, Q et R résultent alors d'une division euclidienne.

Ⓒ 2- <u>Premier corollaire</u> : <u>Soient $A, B, P_0 \in K[X]$, P_0 irréductible non facteur de B.</u>
<u>$\forall n \in \mathbb{N}, \exists 1 (Q, R), A = BQ + P_0^n R$, et $\deg Q < n . \deg P_0$, ou $Q = 0$.</u>

Preuve : on applique le théorème précédent, avec $C = P_0^n$, car $P_0^n \wedge B = 1$ ■

<u>Deuxième corollaire</u> : <u>$A, B \in K[X], n \in \mathbb{N}, a \in K$; supposons $B(a) \neq 0$</u>
<u>$\exists 1 (Q, R)$, $A = BQ + (X-a)^n R$, et $\deg Q < n$ ou $Q = 0$.</u>

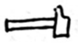
Preuve : c'est le premier corollaire, avec $P_0 = X - a$. ■

Q et R s'appellent dans ce cas « <u>le quotient et le reste de la division "puissances croissantes" de A par B au point a à l'ordre n.</u> »

<u>Troisième corollaire</u> : <u>$A, B \in K[X]$, $val(B) = 0$.</u>
<u>$\forall n \in \mathbb{N}\ \exists 1 (Q, R)$, $A = BQ + X^n R$, et $\deg Q < n$ ou $Q = 0$</u>

Preuve : c'est le corollaire précédent, pour $a = 0$ ■

Dans chaque cas, on dispose d'un algorithme de calcul de Q et R, puisque ce sont des cas particuliers du théorème du 1. Mais cet algorithme "long" est avantageusement remplacé <u>dans le dernier cas</u> par un algorithme beaucoup plus rapide exposé au numéro suivant et qui justifie l'expression de division "puissances croissantes".

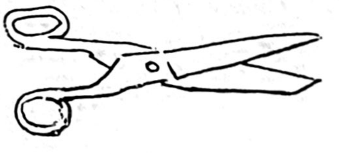

3- <u>Division puissances croissantes</u> : On ordonne A et B puissances <u>croissantes</u>, et on pose la division comme d'habitude, mais en divisant à chaque étape le terme de <u>plus bas</u> degré du reste par le terme de <u>plus bas</u> degré (donc constant) de B. La valuation du reste augmente de 1 au moins à chaque étape. On s'arrête quand elle atteint l'entier n.

Traitons un exemple :

$$
\begin{array}{l|l}
1 + 2X + 3X^2 & 1 - X + X^2 \quad \text{à l'ordre 5} \\
\quad 3X + 2X^2 & \hline 1 + 3X + 5X^2 + 2X^3 - 3X^4 \\
\qquad 5X^2 - 3X^3 & \\
\qquad\quad 2X^3 - 5X^4 & \\
\qquad\qquad -3X^4 - 2X^5 & \\
\qquad\qquad\quad -5X^5 + 3X^6 &
\end{array}
$$

soit : $\underbrace{1 + 2X + 3X^2}_{A} = \underbrace{(1 - X + X^2)}_{B}\underbrace{(1 + 3X + 5X^2 + 2X^3 - 3X^4)}_{Q} + X^5\underbrace{(-5 + 3X)}_{R}$

4 - Cet algorithme est tellement plus efficace que l'autre, que même lorsqu'on se trouve dans le cas du deuxième corollaire (qu'on emploiera par exemple au chapitre 7, §C), on a souvent intérêt à "changer de variable" pour l'appliquer (c'est-à-dire poser $Y = X - a$ et calculer dans $K[Y]$ au lieu de $K[X]$; on passe de l'un à l'autre par exemple par l'identité de Taylor 4-B-3).

(Un autre algorithme  efficace)

CHAPITRE 6 : APPLICATION AUX ÉQUATIONS ALGÉBRIQUES

« Au XVIIIe siècle, Adam Ferguson, philosophe écossais de l'école du "sens commun", prenant au pied de la lettre la "promesse" d'Archimède : « Donnez-moi un point fixe, et je soulèverai la Terre », calcula le temps que mettrait un homme contrebalançant la Terre au bout d'un levier et se déplaçant à la vitesse d'un boulet de canon pour déplacer la Terre d'un pouce.
Le résultat tomba : 44.963.540.000.000 ans. »

(cité de Michel Serres, "Eléments d'histoire des sciences", Paris, 1989)

(A) FACTORISATION ET INTERPOLATION

1 - Par le corollaire 5-A-4, trouver les racines dans K d'un polynôme $P \in K[X]$ revient à trouver les facteurs irréductibles de degré 1 de P.
On ne dispose d'<u>aucun algorithme</u> permettant de le faire pour tout K et pour tout P.

Toutefois, pour $K = \mathbb{Q}$, on a le critère suivant, qui donne toutes les racines rationnelles d'un polynôme $P \in \mathbb{Q}[X]$:

<u>Critère</u> : Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ un polynôme à coefficients <u>entiers</u> (On peut toujours s'y ramener). Alors si $\frac{p}{q}$ est l'expression irréductible d'une racine rationnelle de P, <u>p divise a_0</u> <u>et q divise a_n</u>.

Preuve : le théorème de Gauss appliqué à $q^n P(\frac{p}{q}) = 0$ ■

Il suffira donc d'"essayer" un nombre fini de valeurs possibles.

<u>Exemples</u> : • $P_1(X) = X^3 - 35X^2 + 31X + 2$; $p | 2$ et $q | 1$, donc $\frac{p}{q} = \pm 2, \pm 1$.
Aucune de ces valeurs ne convient, donc P_1 n'a aucune racine rationnelle, et par suite il est irréductible sur $\mathbb{Q}$.

• $P_2(X) = X^3 - 35X^2 + 31X + 3$; $p | 3$ et $q | 1$, donc $\frac{p}{q} = \pm 3, \pm 1$. Seul 1 convient, d'où $P_2(X) = (X-1)(X^2 - 34X - 3)$ où le trinôme, n'ayant plus la racine 1, est irréductible sur $\mathbb{Q}$. (par contre sur $\mathbb{R}$, $X^2 - 34X - 3 = (X - 17 - \sqrt{292})(X - 17 + \sqrt{292})$.)

2 - On a, avec l'algorithme d'Euclide, un procédé <u>systématique</u> pour calculer le pgcd de deux polynômes. Mais ce n'est pas forcément le plus efficace. On peut remarquer que <u>les facteurs irréductibles du pgcd sont les facteurs irréductibles communs aux deux polynômes</u> ; en particulier <u>les racines du pgcd sont les racines communes aux deux polynômes</u>. (cf. les formules du 5-B-3). Si donc on connaît la factorisation irréductible de l'un des deux, il suffit de tester la divisibilité de l'autre par chaque facteur pour déterminer ceux du pgcd.

Exemple: Calculer le pgcd de $A = X^4 + X^3 + 2X^2 + X + 1$ et $B = X^{15.000} + X^7 - X^3 - X + 1$.
Les racines complexes de $A = (X^2+X+1)(X^2+1)$ sont $i, -i, j$ et j^2.
Or $B(i) = 0 - i + i - i + 1 \neq 0$, donc $B(-i) \neq 0$, tandis que $B(j) = 0 + j - 1 - j + 1 = 0 = B(j^2)$.
Par 5-A-4, B est divisible par $X-j$ et par $X-j^2$, donc (Gauss) par $(X-j)(X-j^2) = X^2+X+1$, tandis que ni $X-i$, ni $X+i$, ni a fortiori X^2+1 ne divisent B.
D'où $A \wedge B = X^2+X+1$.
La réponse vaut a priori dans $\mathbb{C}[X]$, mais comme A, B et X^2+X+1 sont dans $\mathbb{Q}[X]$, le résultat est le même dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, et même $K[X]$ dès que K est de caractéristique nulle ! (l'algorithme d'Euclide donnerait toujours les mêmes coefficients rationnels).

3 - **Proposition:** Un polynôme $P \in K[X]$ de degré $p \in \mathbb{N}^*$ a au plus p racines distinctes.

Preuve: Soient $a_1, \ldots, a_n \in K$ n racines distinctes de P. Par 5-A-4, P est divisible par $X-a_1$, par $X-a_2$, .., par $X-a_n$; donc par le théorème de Gauss, il l'est par $(X-a_1)(X-a_2)$, puis par $(X-a_1)(X-a_2)(X-a_3)$, .., et finalement par $(X-a_1)(X-a_2)\cdots(X-a_n)$, puisque $(X-a_n) \wedge (X-a_1)\cdots(X-a_{n-1}) = 1$, car $(a_n - a_1)\cdots(a_n - a_{n-1}) \neq 0$ (cf. le 2). Donc $P = \prod_{j=1}^{n}(X-a_j) \cdot Q$ pour un certain $Q \neq 0$, d'où $\deg P \geq n$. ■

En particulier un polynôme non nul n'a qu'un nombre fini de racines. Il s'ensuit que dès que K est infini l'application $P \mapsto \tilde{P}$, qui à un polynôme associe la fonction polynôme correspondante, est injective.
Preuve: $\tilde{P} = \tilde{Q} \Rightarrow \widetilde{P-Q} = \tilde{P} - \tilde{Q}$ s'annule en tout point de $K \Rightarrow P - Q = 0$ ■

Par contre, il existe toujours un polynôme de degré $\leq p$ ayant pour racines p nombres donnés distincts $a_1, \ldots, a_p \in K$: il est en fait de degré p exactement, et c'est n'importe quel polynôme de la forme $P = c \prod_{j=1}^{p}(X-a_j)$, avec $c \in K$. (cf la preuve de la proposition).

4 - **Proposition:** Il existe un seul polynôme $P \in K[X]$ de degré $< p$, qui prend p valeurs données $b_1, \ldots, b_p \in K$ en p points donnés distincts $a_1, \ldots, a_p \in K$.

Preuve: L'unicité résulte du 3, l'existence, de la formule suivante, appelée "Formule d'interpolation de Lagrange"

$$(*) \qquad \boxed{P(X) = \sum_{j=1}^{p} b_j \left(\prod_{k \neq j} \frac{(X-a_k)}{(a_j - a_k)} \right)} \qquad ■$$

On a couramment besoin, dans les sciences expérimentales, d'"interpoler", c'est-à-dire de trouver une fonction simple dont le graphe passe par un nombre fini p de points donnés (résultats de mesures, par exemple). La formule de Lagrange (*) fournit une solution polynôme, de degré minimal.

Exemple : Déterminer le seul polynôme P de degré 2 tel que $P(0)=1$, $P(1)=2$, $P(2)=4$.

(*) s'écrit ici $P = 1.\frac{(X-1)(X-2)}{(0-1)(0-2)} + 2.\frac{(X-0)(X-2)}{(1-0)(1-2)} + 4.\frac{(X-0)(X-1)}{(2-0)(2-1)} = \frac{1}{2}X^2 + \frac{1}{2}X + 1$.

Remarque : $P(3) = 7$, et non pas 8 !

(B) RACINES MULTIPLES

1- On rappelle que $a \in K$ est dit racine de $P \in K[X]$ de multiplicité (ou ordre) m si $(X-a)^m \mid P$, et $(X-a)^{m+1} \nmid P$. Une racine est dite simple, double, triple, ..., multiple selon que m vaut $1, 2, 3, \dots, >1$.

Dans $\mathbb{C}[X]$ en particulier, si un polynôme admet pour seules racines $a_1, \dots, a_p \in \mathbb{C}$, de multiplicités $m_1, \dots, m_p$, c'est que $P = c\prod_{j=1}^{p}(X-a_j)^{m_j}$, avec $c \in \mathbb{C}^*$, et par suite $\deg P = \sum_{j=1}^{p} m_j$.

Autrement dit un polynôme à coefficients complexes de degré $p>0$ admet exactement p racines « comptées avec leur multiplicité ».

2- Lorsque K est de caractéristique nulle, un critère simple permet de déterminer s'il existe des racines multiples, et éventuellement de les calculer.

Proposition : $P \in K[X]$, $a \in K$, $m \in \mathbb{N}$, carac $K = 0$. Alors
a racine de multiplicité $\geq m \iff$ a racine commune de $P, P', \dots, P^{(m-1)}$

Preuve : $\Leftarrow$ résulte de l'identité de Taylor 4-B-3 ; $\Rightarrow$ de la formule de Leibniz appliquée à $P = (X-a)^m Q$. ∎

Remarque : En fait on peut montrer, en utilisant la formule de Leibniz et le théorème de Gauss, que plus généralement dès que P_0 est un irréductible : $P_0^m \mid P \iff P_0$ divise $P, P', \dots, P^{(m-1)}$ (toujours pour carac $K=0$)

3- Les racines multiples (= au moins doubles) de P sont donc les racines communes à P et P', et par A-2, ce sont les racines de $P \wedge P'$, qui est de degré plus petit... Cela donne une méthode de calcul des racines multiples, qu'on va illustrer ici sur trois exemples :

Exemple 1 : La dérivée de $P = X^4 + 7X^3 + 17X^2 + 17X + 6$ est $4X^3 + 21X^2 + 34X + 17$, et le pgcd, calculé par l'algorithme d'Euclide vaut $X+1$. Donc P est divisible par $(X+1)^2$. On trouve $P = (X+1)^2(X+2)(X+3)$, et on a ainsi obtenu la décomposition irréductible de P.

Exemple 2 : A quelles conditions sur $\lambda, \mu \in \mathbb{C}$, le polynôme $P = X^4 - 2\lambda X^2 + \mu$ a-t-il des racines multiples ? Comme $P' = 4X^3 - 4\lambda X = 4X(X^2 - \lambda)$ a les racines 0 et $\pm\sqrt{\lambda}$,
- si $\mu = 0$, 0 est racine double (même quadruple si $\lambda = 0$ aussi)
- si $\mu = \lambda^2$, les deux racines carrées de λ sont racines doubles.
- dès que $\mu \neq 0, \lambda^2$, P a quatre racines simples.

Exemple 3 : Racines multiples de l'équation réduite du troisième degré :

$X^3+pX+q=0$ $(p,q\in\mathbb{C})$. $P=X^3+pX+q$, $P'=3X^2+p$ de racines $\pm\sqrt{-\frac{p}{3}}$, qui sont racines de P si et seulement si $\pm\sqrt{-\frac{p}{3}}\left(-\frac{p}{3}+p\right)=-q \Leftrightarrow \boxed{4p^3+27q^2=0}$, la racine multiple étant alors $-\frac{3q}{2p}=\frac{2p^2}{9q}$, comme on le voit par exemple en calculant $P\wedge P'$ par l'algorithme d'Euclide ; et cette remarque permet une factorisation complète explicite de P.

(C) RELATIONS ENTRE COEFFICIENTS ET RACINES

1- On se place ici dans $\mathbb{C}[X]$, de sorte qu'un polynôme $P=a_0X^n+a_1X^{n-1}+\dots+a_n$ de degré n $(a_0\neq 0)$ a toujours exactement n racines $\alpha_1,\dots,\alpha_n\in\mathbb{C}$, distinctes ou non, comptées avec leurs multiplicités : $P=a_0(X-\alpha_1)\dots(X-\alpha_n)$.

Développant la deuxième expression de P et l'identifiant à la première, il vient :

$$(*)\quad \boxed{\sigma_j=\frac{(-1)^j a_j}{a_0}} \text{ pour } j=1,\dots,n, \text{ avec } \boxed{\sigma_j=\sum_{1\le i_1<\dots<i_j\le n}\alpha_{i_1}\dots\alpha_{i_j}}\quad (**)$$

Réciproquement, n nombres complexes donnés $\alpha_1,\dots,\alpha_n$ distincts ou non, sont les racines, avec multiplicités, du polynôme de degré n

$$\boxed{P=X^n+\sum_{j=1}^{n}(-1)^j\sigma_j X^{n-j}}\qquad (***)$$

Les relations $(*)$ sont les "relations entre coefficients et racines", les σ_j définis par $(**)$ s'appellent "fonctions symétriques élémentaires" des n nombres $\alpha_1,\dots,\alpha_n$ ("symétriques" signifiant : invariantes par une permutation arbitraire de ces nombres). Par exemple les fonctions symétriques élémentaires de trois nombres a,b,c (pas forcément distincts) sont $\sigma_1=a+b+c$, $\sigma_2=ab+bc+ac$, $\sigma_3=abc$.

Enfin la formule $(***)$ permet d'écrire l'équation dont n nombres donnés sont les racines (distinctes ou non), et on retrouve ainsi par exemple que deux nombres de somme s et de produit p sont les racines de $X^2-sX+p=0$ (cf. 2-B-1) ; voir aussi le calcul de $\cos\frac{2\pi}{7}$ à la fin de 2-B-6.

2- **Exemple :** Trouver trois nombres complexes z_1,z_2,z_3 de module 1, de somme 1, et de produit 1. On a donc $z_1+z_2+z_3=1$, $z_1z_2z_3=1$, et comme $|z_1|=|z_2|=|z_3|=1$, il vient aussi $z_1z_2+z_2z_3+z_1z_3=\frac{1}{z_3}+\frac{1}{z_1}+\frac{1}{z_2}=\bar z_3+\bar z_1+\bar z_2=\overline{z_1+z_2+z_3}=\bar 1=1$, et z_1,z_2,z_3 sont les trois racines de $X^3-X^2+X-1=(X-1)(X^2+1)$, soit $1, i$, et $-i$ ■

Il est important de remarquer que ces "relations entre coefficients et racines permettent de calculer certaines fonctions des racines d'une équation connue, même lorsqu'on ne sait pas calculer ces racines :

Exemple : Calculer $S=\alpha_1^2+\dots+\alpha_5^2$, où $\alpha_1,\dots,\alpha_5$ sont les racines complexes de $X^5-4X^4+eX^3-\pi X^2+37X-19+300.000i=0$

En fait $S=(\alpha_1+\dots+\alpha_5)^2-2(\alpha_1\alpha_2+\dots+\alpha_4\alpha_5)=\sigma_1^2-2\sigma_2$.

Comme, par $(*)$ $\sigma_1=4$ et $\sigma_2=e$, il vient $S=16-2e$ ■

3- Quelles fonctions de $\alpha_1, \dots, \alpha_n$ peut-on ainsi calculer? La réponse est le <u>théorème de Newton</u> suivant, que nous <u>admettrons</u> ici (il se démontre par une multiple récurrence assez compliquée):

<u>Théorème</u>: Si $P \in K[X_1, \dots, X_n]$ <u>est symétrique</u> (= invariant par permutation des variables), <u>il existe $Q \in K[X_1, \dots, X_n]$ tel que $P(\alpha_1, \dots, \alpha_n) = Q(\sigma_1, \dots, \sigma_n)$</u>.

En particulier $S_p = \sum_{j=1}^{n} \alpha_j^p$ est un tel polynôme symétrique, et des "Formules de Newton" donnent les S_p ($p \in \mathbb{N}$) explicitement comme polynômes des σ_j ($1 \le j \le n$). On se contentera ici de calculer un exemple simple.

<u>Exemple</u>: Si λ et μ sont deux nombres de somme s et de produit p,
$\lambda^3 + \mu^3 = (\lambda+\mu)^3 - 3\lambda^2\mu - 3\lambda\mu^2 = (\lambda+\mu)^3 - 3\lambda\mu(\lambda+\mu) = s^3 - 3ps$.

(D) DERNIÈRES REMARQUES SUR LA DIVISION

1- La "théorie de la division" est exactement la même dans les anneaux $\mathbb{Z}$ (chap. 1) et $K[X]$ (chap. 5). Le résultat crucial est que: (*) <u>tout idéal est monogène</u>. On reprendra au chapitre 18 la même théorie dans un cadre un peu plus général. Rappelons-en le schéma: on commence par démontrer un théorème de <u>division euclidienne</u>, dont on déduit (*); d'où l'existence et les propriétés des <u>pgcd</u> et <u>ppcm</u>, et l'identité de <u>Bezout</u> qui sert à démontrer le théorème de <u>Gauss</u>. Enfin on se sert de celui-ci pour obtenir le théorème de <u>décomposition</u> en facteurs "premiers" ou "irréductibles". Notons enfin que toutes les démonstrations sont truffées de raisonnements par récurrence (sur les degrés dans le cas de $K[X]$.)

δ] Si l'on ne fait pas la même théorie pour les polynômes de <u>plusieurs</u> variables, c'est qu'elle est <u>fausse</u>. Le théorème de décomposition reste vrai, et il y a toujours des pgcd et ppcm, mais l'identité de Bezout disparaît, car certains idéaux ne sont <u>pas</u> monogènes:
Exemple: Dans l'anneau $K[X,Y]$, les polynômes X et Y engendrent l'idéal $I = \langle X, Y \rangle = \{P \in K[X,Y] \mid P(0,0) = 0\}$. Comme ils sont irréductibles, $X \wedge Y = 1$; or $I \neq \langle 1 \rangle = K[X,Y]$. ■

2- De même qu'on a muni le quotient $\mathbb{Z}/n$ de $\mathbb{Z}$ par la relation "modulo n" d'une structure d'anneau héritée de celle de $\mathbb{Z}$, on peut considérer, pour $P_0 \in K[X]$ donné, la relation d'équivalence $P \sim Q \Leftrightarrow P_0 \mid P - Q$, et munir l'ensemble-quotient $K[X]/_{P_0}$ d'une structure d'anneau commutatif unitaire en posant $\dot{P} + \dot{Q} = \widehat{P+Q}$ et $\dot{P}\dot{Q} = \widehat{PQ}$ (après avoir vérifié que les classes de $P+Q$ et de PQ ne dépendent que de celles de P et de Q).

On aura alors l'énoncé suivant, analogue de 1-D-3:

<u>Proposition</u>: $K[X]/_{P_0}$ <u>intègre</u> $\Leftrightarrow$ $K[X]/_{P_0}$ <u>corps</u> $\Leftrightarrow$ P_0 <u>irréductible</u>

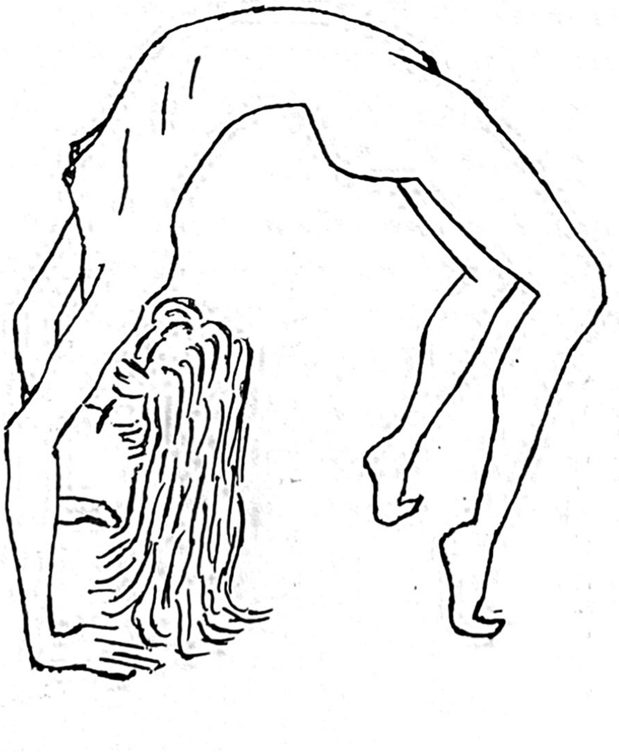
Preuve : Supposons $K[X]/_{P_0}$ intègre. Alors P_0 est irréductible, car sinon $P_0 = P_1 P_2$ avec $\dot{P}_1 \neq \dot{0}$, $\dot{P}_2 \neq \dot{0}$, et partant $\dot{P}_1 \dot{P}_2 = \dot{P}_0 = \dot{0}$. Si maintenant P_0 est irréductible, et $\dot{P} \in K[X]/_{P_0} - \{\dot{0}\}$, P n'est pas divisible par P_0, donc $P_0 \wedge P = 1$ et il existe Q et $R \in K[X]$ tels que $PQ + P_0 R = 1$, d'où $\dot{1} = \dot{P}\dot{Q} + \dot{0}$, et $\dot{P}$ est inversible. Donc $K[X]/_{P_0}$ est un corps. Enfin tout corps est intègre. ■

3° Supposons P_0 irréductible unitaire, et posons $\overline{K} = K[X]/_{P_0}$. Comme $\deg P_0 \geqslant 1$, l'application $\begin{array}{c} K \longrightarrow \overline{K} \\ a \longmapsto \dot{a} \end{array}$ est injective, et K s'identifie à un <u>sous-corps</u> du corps $\overline{K}$. On a donc fabriqué ainsi à partir d'un premier corps de nombres K (commutatif), un corps commutatif $\overline{K}$ plus grand, appelé une "<u>extension algébrique</u>" de K.

Cette construction ne donne <u>rien</u> de nouveau lorsque $\deg P_0 = 1$, disons par $P_0 = X - c$, car l'application $K \to \overline{K}$ est <u>bijective</u> dans ce cas (comme représentant canonique d'un élément $\dot{P}$ de $\overline{K}$, on peut prendre le reste de la division de P par $X-c$, qui est la constante $P(c)$.)
Par exemple, il est impossible de plonger $\mathbb{C}$ dans un corps plus grand par ce procédé d'"extension algébrique". On n'obtiendra une vraie extension de K que si $K[X]$ possède des irréductibles de degré > 1.

Les extensions de $\mathbb{Q}$ qu'on peut construire ainsi sont les "corps de nombres algébriques". Quant à $\mathbb{R}$, il a des irréductibles de degré 2, de la forme $X^2 + aX + b$, avec $a, b \in \mathbb{R}$, $a^2 - 4b < 0$.

Pour $b = 1$ et $a = 0$ par exemple, $\overline{\mathbb{R}} = \mathbb{R}[X]/_{X^2+1}$ n'est autre que le corps $\mathbb{C}$ des nombres complexes ! (on note $\dot{X} = i$).
C'est d'ailleurs essentiellement la seule extension algébrique de $\mathbb{R}$, car $X^2 + aX + b = (X + \frac{a}{2})^2 + c^2$, avec $c = \sqrt{b - \frac{a^2}{4}}$, et on a des isomorphismes d'anneaux évidents : $\mathbb{R}[cX] \simeq \mathbb{R}[X] \simeq \mathbb{R}[X + \frac{a}{2}]$. ⌋⌋



(Extension qui n'a rien d'algébrique)

CHAPITRE 7 : LE CORPS DES FRACTIONS RATIONNELLES

« Les atomes restent ensemble jusqu'au temps où une quelconque nécessité plus forte vient du dehors, et les secoue, et les disperse. »
(Simplicius, commentaire à Aristote)

(A) FRACTIONS RATIONNELLES ET FONCTIONS RATIONNELLES

1- Les entiers ne formant pas un corps (seuls 1 et -1 sont inversibles dans $\mathbb{Z}$), on les a plongés en 2-A-1 dans le corps $\mathbb{Q}$ des rationnels en "inventant" leurs inverses $\frac{1}{q}$, puis les multiples de ces inverses $\frac{p}{q}$... mais en prenant garde que, comme $\frac{p}{q}$ n'a d'autre sens que "quelqu'un qui multiplié par q vaut p", nécessairement $\frac{p}{q}=\frac{p'}{q'}$ dès que $pq'=p'q$. Les seuls polynômes inversibles étant les constantes non nulles, on va de même plonger l'anneau intègre $K[X]$ dans un corps plus grand, par la même construction.

On considère donc l'ensemble-quotient $E = K[X]\times K[X]^*/_\sim$, où l'équivalence est définie par $(P,Q)\sim(P',Q') \Leftrightarrow PQ'=P'Q$. La classe de (P,Q) sera notée $\frac{P}{Q}$ (donc $\frac{P}{Q}=\frac{P'}{Q'} \Leftrightarrow PQ'=P'Q$), on identifie $K[X]$ à une partie de E par $P\mapsto \frac{P}{1}$ (qui est une injection, car $K[X]$ est intègre), et si l'on veut définir sur E une somme et un produit (associatifs, commutatifs, et distributif) qui prolongent les opérations de $K[X]$, il faut bien poser :

$\frac{P}{Q}+\frac{P'}{Q'} = \frac{PQ'+P'Q}{QQ'}$ (puisque $QQ'\left(\frac{P}{Q}+\frac{P'}{Q'}\right) = Q'\cdot\left(Q\cdot\frac{P}{Q}\right)+Q\cdot\left(Q'\cdot\frac{P'}{Q'}\right) = PQ'+P'Q$)

et $\frac{P}{Q}\cdot\frac{P'}{Q'} = \frac{PP'}{QQ'}$ (puisque... ; notons que ces formules n'ont de sens que parce que $Q\neq 0$ et $Q'\neq 0 \Rightarrow QQ'\neq 0$, par intégrité)

Il est facile de vérifier que E, muni de ces deux opérations, est encore un anneau unitaire commutatif, où $0=\frac{0}{1}$, $-\left(\frac{P}{Q}\right)=\frac{-P}{Q}$, $1=\frac{1}{1}$, et $\frac{P}{Q}=0 \Leftrightarrow P=0$. Mais de plus tout élément non nul de E est inversible : $\left(\frac{P}{Q}\right)^{-1}=\frac{Q}{P}$.
Muni de ces opérations, E est donc un corps commutatif, qu'on appelle le corps des fractions rationnelles (à coefficients dans K), et qu'on note $K(X)$.

Comme, pour tous $P, Q\neq 0, R\neq 0$, $\frac{PR}{QR}=\frac{P}{Q}$, on peut remarquer dans chaque classe $\frac{P}{Q}$ un représentant canonique, l'expression irréductible de la fraction rationnelle, celle pour laquelle $P\wedge Q=1$ (et de plus Q unitaire, par exemple.)

2- A toute fraction rationnelle $\frac{P}{Q}$ (supposons $P\wedge Q=1$), on peut associer une application à valeurs dans K, la fonction rationnelle associée $x\mapsto \frac{P(x)}{Q(x)}$ définie pour $x\in K$ dès que $Q(x)\neq 0$, autrement dit sur K privé de l'ensemble (fini) des racines de Q, qu'on appelle pôles de la fraction $\frac{P}{Q}$. Cette correspondance n'est bijective que si K est infini (même argument qu'en 6-A-3).

3- La <u>dérivation</u> formelle des polynômes se prolonge aux fractions rationnelles : c'est <u>la seule application $K(X) \to K(X)$ qui étend la dérivation des polynômes, et telle que : $\forall R, S \in K(X)$, $(RS)' = R'S + RS'$.</u>

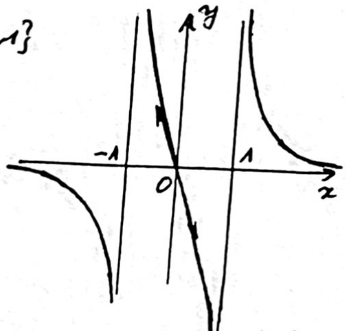
En effet on aura nécessairement, pour $P, Q \in K[X]$, $Q \neq 0$:

$$Q' \cdot \frac{1}{Q} + Q \cdot \left(\frac{1}{Q}\right)' = \left(Q \cdot \frac{1}{Q}\right)' = 1' = 0 \text{, d'où } \left(\frac{1}{Q}\right)' = \frac{-Q'}{Q^2} \text{, puis } \left(\frac{P}{Q}\right)' = \left(P \cdot \frac{1}{Q}\right)' = \frac{P'}{Q} - \frac{PQ'}{Q^2},$$

et donc toutes les formules habituelles, par exemple :

$$\boxed{\left(\frac{P}{Q}\right)' = \frac{QP' - PQ'}{Q^2},\ \left(\frac{P}{Q^m}\right)' = \frac{QP' - mPQ'}{Q^{m+1}},\ (R^m)' = mR^{m-1}R'} \quad (m \in \mathbb{Z}, R \in K[X])$$

4- La fonction $x \overset{f}{\mapsto} \dfrac{2x}{x^2-1}$ est indéfiniment dérivable sur $\mathbb{R} - \{-1, 1\}$.



(allure du graphe)

Par exemple $f'(x) = \dfrac{-2(x^2+1)}{(x^2-1)^2}$, $f''(x) = \dfrac{\cdots}{(x^2-1)^3}$, …

Mais peut-on calculer explicitement la dérivée <u>n-ième</u> de f ?

Oui, car $\left(\dfrac{1}{x+1}\right)^{(n)} = \left((x+1)^{-1}\right)^{(n)} = (-1)(-2)\cdots(-n)(x+1)^{-1-n} \cdot 1 = \dfrac{(-1)^n n!}{(x+1)^{n+1}}$

d'où $f^{(n)}(x) = \left(\dfrac{1}{x+1} + \dfrac{1}{x-1}\right)^{(n)} = (-1)^n n! \left(\dfrac{1}{(x+1)^{n+1}} + \dfrac{1}{(x-1)^{n+1}}\right)$

$$= \frac{2(-1)^n n!}{(x^2-1)^{n+1}} \left(\sum_{j=0}^{\left[\frac{n+1}{2}\right]} C_n^{2j} x^{n+1-2j} \right)$$

C'est <u>parce</u> qu'on a su décomposer f en somme de fractions plus simples qu'on y est arrivé. C'est aussi le procédé qui permet de calculer les <u>primitives</u> des fonctions rationnelles : on sait le faire lorsqu'elles sont assez "simples", et on peut s'y ramener grâce au théorème du paragraphe suivant.

(B) DÉCOMPOSITION EN ÉLÉMENTS SIMPLES

1- On dit qu'une fraction $R = \dfrac{P}{Q} \in K(X)$ est <u>propre</u> lorsque $\deg P < \deg Q$, ou $P = 0$ (ce qui ne dépend pas du représentant choisi). Une somme de fractions propres est propre ; un produit encore plus.

On appelle <u>élément simple</u> de $K(X)$ toute fraction de la forme $\dfrac{P}{Q_0^n}$ avec $n \in \mathbb{N}^*$, Q_0 <u>irréductible</u> (unitaire) et <u>$\deg P < \deg Q_0$</u> (en particulier, c'est une fraction propre !).

Par exemple dans $\mathbb{C}[X]$, les éléments simples sont les fractions de la forme $\dfrac{A}{(X-a)^n}$ $(a, A \in \mathbb{C}, n \in \mathbb{N}^*)$, tandis que dans $\mathbb{R}[X]$, il y en a de deux sortes : $\dfrac{A}{(X-a)^n}$ $(a, A \in \mathbb{R}, n \in \mathbb{N}^*)$, et $\dfrac{AX+B}{(X^2+aX+b)^n}$ $(a, b, A, B \in \mathbb{R}, a^2 - 4b < 0, n \in \mathbb{N}^*)$. Dans $\mathbb{Q}(X)$, il y en aurait encore beaucoup d'autres.

2- Théorème (de "décomposition en éléments simples")

Soit $R = \frac{P}{Q} \in K(X)$, et supposons l'expression irréductible ($P \wedge Q = 1$, Q unitaire). Soit $Q = B_1^{m_1} \cdots B_q^{m_q}$ la décomposition de Q en facteurs irréductibles unitaires distincts ($B_j \neq B_k$). Il existe une et une seule écriture de R de la forme

$$(*) \qquad \boxed{R = E + \sum_{j=1}^{q} \left(\sum_{i=1}^{m_j} \frac{A_{ji}}{B_j^i} \right)}$$

où E et les $A_{ji} \in K[X]$, $\deg A_{ji} < \deg B_j$ (les $\frac{A_{ji}}{B_j^i}$ sont des éléments simples). E s'appelle la partie entière de R ; $E = 0$ si et seulement si R est propre, sinon $\deg E = \deg P - \deg Q$. La j-ème parenthèse $R_j = \sum_{i=1}^{m_j} \frac{A_{ji}}{B_j^i}$ s'appelle la partie polaire de R relative au facteur B_j
(Si $B_j = X - a_j$, on dit que a_j est un pôle de R de multiplicité m_j).

Preuve: D'abord la somme des parties polaires est une fraction propre $\frac{P_1}{Q}$, donc $P = EQ + P_1$ avec $\deg P_1 < \deg Q$ ou $P_1 = 0$, et nécessairement E et P_1 sont le quotient et le reste de la division euclidienne de P par Q. Donc E est bien déterminée, nulle si R était propre, et $R - E$ est propre. On peut donc supposer R propre dans la suite, et $E = 0$.

Appliquons le "Premier Corollaire" du 5-C-2, avec ici $A = P$, $B = \prod_{k \neq j} B_k^{m_k}$, $P_0 = B_j$ et $n = m_j$. Il vient un et un seul couple (P_j, S) tel que
$P = \left(\prod_{k \neq j} B_k^{m_k} \right) P_j + B_j^{m_j} S$, avec $\deg P_j < m_j \deg B_j$ ou $P_j = 0$,
d'où $R = \frac{P}{Q} = \frac{P_j}{B_j^{m_j}} + \frac{S}{\prod_{k \neq j} B_k^{m_k}}$, où toutes les fractions écrites sont propres,
et le dénominateur de la dernière n'a plus le facteur B_j. Par récurrence sur le nombre q de facteurs irréductibles du dénominateur, il est donc clair qu'il existe une et une seule façon d'écrire $R = \sum_{j=1}^{q} R_j$, avec $R_j = \frac{P_j}{B_j^{m_j}}$, et $\deg P_j < m_j \deg B_j$ ($P_j = 0$ impliquerait que Q n'avait pas le facteur B_j).

Enfin on voit que chaque partie polaire R_j se décompose de façon unique en somme d'éléments simples:
$$R_j = \sum_{i=1}^{m_j} \frac{A_{ji}}{B_j^i} \iff P_j = A_{j,m_j} + A_{j,m_j-1} B_j + \cdots + A_{j,1} B_j^{m_j-1},$$
par divisions euclidiennes successives de P_j par $B_j^{m_j-1}$, du reste par $B_j^{m_j-2}$ ... ■

3 - La preuve fournit en même temps un algorithme complet de calcul de la décomposition, puisque chaque division invoquée, et même le corollaire 5-C-2, sont déjà "algorithmiques". La seule partie du calcul où un algorithme fait défaut est la décomposition initiale du dénominateur de R en facteurs irréductibles. On est donc certain de savoir calculer la décomposition en éléments simples d'une fraction donnée dès qu'on a su factoriser complètement le dénominateur, et seulement dans ce cas.

Mais les algorithmes invoqués, en particulier celui du 5-C-2, sont longs et compliqués, et la pratique de la décomposition des fractions rationnelles joue de préférence sur un répertoire de méthodes non systématiques, mais suffisantes pour traiter les fractions "pas trop" compliquées.

Les plus classiques de ces méthodes sont décrites au paragraphe suivant. Elles se fondent sur la remarque que, puisque la décomposition cherchée est <u>unique</u>, dès qu'on a réussi à écrire R sous la forme voulue (*), c'est la bonne décomposition. On ne traitera que des cas $K=\mathbb{C}$ et $K=\mathbb{R}$, utiles en calcul intégral.

(C) PRATIQUE DE LA DÉCOMPOSITION ($K=\mathbb{R}$ ou $\mathbb{C}$)

1- Il est bon de commencer par écrire la forme exacte de la décomposition cherchée, avec des constantes inconnues qu'on déterminera ensuite. Par exemple:

$$R(X)=\frac{X^6}{X^4+2X^3+2X^2+2X+1}=\begin{cases} aX^2+bX+c+\dfrac{d}{(X+1)^2}+\dfrac{e}{X+1}+\dfrac{f}{X-i}+\dfrac{g}{X+i} & (\text{sur } \mathbb{C}) \\ a'X^2+b'X+c'+\dfrac{d'}{(X+1)^2}+\dfrac{e'}{X+1}+\dfrac{f'X+g'}{X^2+1} & (\text{sur } \mathbb{R}) \end{cases}$$

$(\in \mathbb{Q}(X)\subset\mathbb{R}(X)\subset\mathbb{C}(X))$

Comme les algorithmes de division calculent dans $\mathbb{Q}(X)$, on a forcément $a'=a$, $b'=b$, $c'=c$, $d'=d$, $e'=e$. De plus $\frac{f}{X-i}+\frac{g}{X+i}=\frac{(f+g)X+i(f-g)}{X^2+1}$,

et en comparant les deux expressions de la même fraction de $\mathbb{C}(X)$, il vient $f+g=f'$ et $i(f-g)=g'$ (d'où aussi $f',g'\in\mathbb{R}\Rightarrow f$ et g complexes conjugués !)

On voit sur cet exemple que les décompositions sur $\mathbb{R}$ et sur $\mathbb{C}$ d'une même fraction de $\mathbb{R}(X)$, bien que distinctes, se déduisent facilement l'une de l'autre.

En particulier si $R\in\mathbb{R}(X)$, les parties polaires relatives aux pôles complexes conjugués de sa décomposition sur $\mathbb{C}$ sont complexes conjuguées, et en "réduisant au même dénominateur", elles donnent les parties polaires sur $\mathbb{R}$ relatives aux facteurs irréductibles de degré 2 ; c'est d'ailleurs souvent la meilleure façon de calculer ces dernières, surtout dans le cas de pôles simples.

2- La partie entière se calcule par division euclidienne. Dans l'exemple ci-dessus:

X^6	$X^4+2X^3+2X^2+2X+1$
$-2X^5-2X^4-2X^3-X^2$	X^2-2X+2
$2X^4+2X^3+3X^2+2X$	
$-2X^3-X^2-2X-2$	

d'où $$\frac{X^6}{X^4+2X^3+2X^2+2X+1}=X^2-2X+2-\frac{2X^3+X^2+2X+2}{(X+1)^2(X^2+1)}$$

3- Les "<u>termes dominants</u>" sont ceux de la forme $\frac{A_{j,m_j}}{(X-a_j)^{m_j}}$; on les calcule facilement en multipliant tout par $(X-a_j)^{m_j}$, puis substituant a_j à X.

Dans l'exemple ci-dessus, les "coefficients dominants" de la décomposition sur $\mathbb{C}$ sont d, f, et g:

$(X+1)^2R=(X+1)(\cdots)+d$, d'où pour $X=-1$, $\frac{(-1)^6}{((-1)^2+1)}=0+d$, soit $d=\frac{1}{2}$

$(X-i)R=(X-i)(\cdots)+f$, d'où pour $X=i$

$\frac{i^6}{(i+1)^2(i+i)}=0+f$, soit $f=\frac{1}{4}$, puis aussi $g=\overline{f}=\frac{1}{4}$.

C'est ici la façon la plus simple de calculer aussi $f'=f+g=\frac{1}{2}$ et $g'=i(f-g)=0$.

4 - On peut utiliser d'autres remarques de symétrie pour s'épargner une partie des calculs, et par exemple, un raisonnement de parité si R est paire ou impaire, dont voici le principe, sur un exemple :

$$\frac{1}{X^6-X^4-X^2+1} = \frac{A}{(X-1)^2} + \frac{B}{X-1} + \frac{C}{(X+1)^2} + \frac{D}{X+1} + \frac{E}{X-i} + \frac{F}{X+i} \quad (\text{sur } \mathbb{C})$$

changeons X en $-X$: idem $= \dfrac{A}{(X+1)^2} + \dfrac{-B}{X+1} + \dfrac{C}{(X-1)^2} + \dfrac{-D}{X-1} + \dfrac{-E}{X+i} + \dfrac{-F}{X-i}$.

Par unicité de la décomposition, il vient $A=C$, $B=-D$, et $E=-F$, et il ne reste donc plus que trois constantes à calculer.

5 - On appelle résidus les coefficients A et B dans les termes de la forme $\dfrac{A}{X-a_j}$ et $\dfrac{BX+C}{X^2+a_jX+b_j}$. On a alors, pour une fraction propre seulement $\dfrac{P}{Q}$:

Si $\deg P = \deg Q - 1$, la somme des résidus est le quotient des coefficients des termes de plus haut degré de P et de Q ; si $\deg P \leq \deg Q - 2$, elle est nulle.

Preuve : Si $P(X) = aX^p + \cdots$ et $Q(X) = bX^{p+1} + \cdots$, quand $z \to \infty$, $\dfrac{zP(z)}{Q(z)} \to \dfrac{a}{b}$; or le second membre de (*) tend vers la somme des résidus.
Si la différence des degrés est d'au moins 2, $\dfrac{zP(z)}{Q(z)} \to 0$. ■

Exemple : $\dfrac{2X}{X^4-1} = \dfrac{A}{X-1} + \dfrac{B}{X+1} + \dfrac{CX+D}{X^2+1}$ sur $\mathbb{R}$, donc $A+B+C=0$.
Comme $A = \frac{1}{2}$ (terme dominant), et $B = A = \frac{1}{2}$ (imparité), il vient $C=-1$.
De plus $D=0$ (imparité). Finalement : $\dfrac{2X}{X^4-1} = \dfrac{1/2}{X-1} + \dfrac{1/2}{X+1} - \dfrac{X}{X^2+1}$.

6 - Dernières remarques (illustrées sur les exemples du numéro suivant) :

- Quand il ne reste plus que quelques constantes à calculer (1 ou 2, ou à la rigueur 3), le plus simple est de donner à X autant de valeurs distinctes (et distinctes des pôles), et d'identifier.
- Dès que la fraction a un pôle d'ordre assez élevé (>3 en pratique), la partie polaire correspondante de la décomposition se calcule au plus vite par l'algorithme de division puissances croissantes, après un changement de variable ramenant ce pôle à l'origine (méthode de calcul du 5-C-3 et 4 - voir au 7 ici l'avant-dernier exemple).

7 - Quelques exemples de décomposition

- $\boxed{\dfrac{X^7}{X^3-1}}$

$$\begin{array}{l|l} X^7 & X^3-1 \\ \quad X^4 & X^4+X \\ \quad\quad X & \end{array} \qquad \frac{X^7}{X^3-1} = X^4+X+\frac{X}{X^3-1}$$

$$\frac{X}{X^3-1} = \frac{A}{X-1} + \frac{B}{X-j} + \frac{C}{X-j^2} \qquad A = \frac{1}{1+1+1} = \frac{1}{3}, \quad B = \frac{j}{(j-1)(j-j^2)} = \frac{j}{j^2-j-j^3+j^2} = \frac{j}{3j^2} = \frac{1}{3j} = \frac{j^2}{3}$$

et $C = \overline{B} = \dfrac{j}{3}$, d'où $\dfrac{X^7}{X^3-1} = X^4+X + \dfrac{1/3}{X-1} + \dfrac{j^2/3}{X-j} + \dfrac{j/3}{X-j^2}$ (sur $\mathbb{C}$)

et $\dfrac{j^2/3}{X-j} + \dfrac{j/3}{X-j^2} = \dfrac{\frac{j+j^2}{3}X - \frac{j^4+j^2}{3}}{X^2+X+1} = \dfrac{-\frac{1}{3}X + \frac{1}{3}}{X^2+X+1}$, d'où $\dfrac{X^7}{X^3-1} = X^4+X+\dfrac{1/3}{X-1} - \dfrac{\frac{1}{3}(X-1)}{X^2+X+1}$

(sur $\mathbb{R}$ ... et sur $\mathbb{Q}$).

- $\boxed{\dfrac{X^7}{(X^2-1)^2}} = \cdots = X^3+2X+\dfrac{3X^3-2X}{(X^2-1)^2}$; $\dfrac{3X^3-2X}{(X^2-1)^2} = \dfrac{A}{(X-1)^2}+\dfrac{B}{X-1}+\dfrac{C}{(X+1)^2}+\dfrac{D}{X+1}$

avec $C=-A$ et $D=B$ (imparité), et $B+D=3$ (résidus), d'où $B=D=\frac{3}{2}$, puis $A=\frac{1}{4}$ (dominant), donc $C=-\frac{1}{4}$. Finalement :

$$\frac{X^7}{(X^2-1)^2} = X^3+2X+\frac{1/4}{(X-1)^2}+\frac{3/2}{X-1}-\frac{1/4}{(X+1)^2}+\frac{3/2}{X+1} \quad \text{(sur } \mathbb{R} \text{ et sur } \mathbb{C}\text{)}.$$

- $\boxed{\dfrac{25X^6}{(X^2-4)^2(X^2+1)}} = 25+\dfrac{A}{(X-2)^2}+\dfrac{A'}{X-2}+\dfrac{B}{(X+2)^2}+\dfrac{B'}{X+2}+\dfrac{C}{X-i}+\dfrac{D}{X+i}$ (sur $\mathbb{C}$)

avec $B=A$, $B'=-A'$, $D=-C$ (parité), $D=\overline{C}$ (réalité), puis

$A=\dfrac{25.2^6}{4^2.5}=20=B$, $C=\dfrac{25\,i^6}{(-5)^2 2i}=\dfrac{i}{2}=-D$ (dominants). Pour $X=0$, $0=25+5-\frac{A'}{2}+5-\frac{A'}{2}-\frac{1}{2}-\frac{1}{2}$,

soit $A'=34=-B'$, donc
$$\frac{25X^6}{(X^2-4)^2(X^2+1)} = 25+\frac{20}{(X-2)^2}+\frac{34}{X-2}+\frac{20}{(X+2)^2}-\frac{34}{X+2}+\frac{i/2}{X-i}-\frac{i/2}{X+i} \quad \text{(sur } \mathbb{C}\text{)}$$
$$= \quad " \quad " \quad " \quad " \quad " \quad -\frac{1}{X^2+1} \quad \text{(sur } \mathbb{R}\text{)}.$$

- $\boxed{\dfrac{X^2}{(X^2-1)(X-1)^2}} = \dfrac{A}{(X-1)^3}+\dfrac{B}{(X-1)^2}+\dfrac{C}{X-1}+\dfrac{D}{X+1}$, avec $A=\frac{1}{2}$, $D=-\frac{1}{8}$ (dominants), $C+D=0$

(résidus), donc $C=\frac{1}{8}$. Pour $X=0$, $0=-\frac{1}{2}+B-\frac{1}{8}-\frac{1}{8}$, donc $B=\frac{3}{4}$, et
$$\frac{X^2}{(X^2-1)(X-1)^2} = \frac{1/2}{(X-1)^3}+\frac{3/4}{(X-1)^2}+\frac{1/8}{X-1}-\frac{1/8}{X+1} \quad \text{(sur } \mathbb{R} \text{ et sur } \mathbb{C}\text{)}.$$

- $\boxed{\dfrac{128}{(X-1)^5(X^2-2X+5)}} = \dfrac{A_5}{(X-1)^5}+\dfrac{A_4}{(X-1)^4}+\dfrac{A_3}{(X-1)^3}+\dfrac{A_2}{(X-1)^2}+\dfrac{A_1}{X-1}+\dfrac{B}{X-1-2i}+\dfrac{C}{X-1+2i}$ (sur $\mathbb{C}$)

avec $A_5=32$, $B=-1$, $C=\overline{B}=-1$ (dominants), et $A_1=0-B-C=2$ (résidus).
On est loin du compte et mieux vaut faire la division puissances croissantes :
Si $X=1+Y$, la fraction s'écrit $\dfrac{128}{Y^5(4+Y^2)}=\dfrac{A_5}{Y^5}+\dfrac{A_4}{Y^4}+\dfrac{A_3}{Y^3}+\dfrac{A_2}{Y^2}+\dfrac{A_1}{Y}+$ une fraction sans pôle 0,
donc $128=(A_5+A_4Y+A_3Y^2+A_2Y^3+A_1Y^4)(4+Y^2)+Y^5(\text{polynôme})$

$$\begin{array}{l|l} 128 & 4+Y^2 \\ \hline -32Y^2 & 32-8Y^2+2 \\ \quad 8Y^4 & \end{array}$$
d'où $A_5=32$, $A_4=0$, $A_3=-8$, $A_2=0$, $A_1=2$

et finalement :
$$\frac{128}{(X-1)^5(X^2-2X+5)} = \frac{32}{(X-1)^5}-\frac{8}{(X-1)^3}+\frac{2}{X-1}\begin{cases} -\dfrac{1}{X-1-2i}-\dfrac{1}{X-1+2i} & \text{(sur } \mathbb{C}\text{)} \\ -\dfrac{2(X-1)}{X^2-2X+5} & \text{(sur } \mathbb{R}\text{)}. \end{cases}$$

- $\boxed{\dfrac{X^7}{(X-2)^{1989}}} = \dfrac{128}{(X-2)^{1989}}+\dfrac{448}{(X-2)^{1988}}+\dfrac{672}{(X-2)^{1987}}+\dfrac{560}{(X-2)^{1986}}+\dfrac{280}{(X-2)^{1985}}$
$+\dfrac{84}{(X-2)^{1984}}+\dfrac{14}{(X-2)^{1983}}+\dfrac{1}{(X-2)^{1982}}$ (sur $\mathbb{R}$ et sur $\mathbb{C}$)

(développer $((X-2)+2)^7$ par la formule du binôme).

• D. I. Mendeleiev •